AXIS 221 Network Camera

User's Manual

About this Document

This manual is intended for administrators and users of the AXIS 221 Network Camera, and is applicable for software release 4.45. It includes instructions for using and managing the AXIS 221 on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface.

Safety Notices Used In This Manual

Caution! - Indicates a potential hazard that can damage the product.
Important! - Indicates a hazard that can seriously impair operation.
Do not proceed beyond any of the above notices until you have fully understood the implications.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at http://www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see http://www.opensource.apple.com/apsl/).
The source code is available from:
http://developer.apple.com/darwin/projects/rendezvous/

Legal Considerations

Video surveillance can be prohibited by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

Electromagnetic Compatibility (EMC)

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Re-orient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Connect the equipment to an outlet on a different circuit to the receiver. Consult your dealer or an experienced radio/TV technician for help. Shielded (STP) network cables must be used with this unit to ensure compliance with EMC standards.

USA – This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his/her own expense will be required to take whatever measures may be required to correct the interference.

Canada – This Class B digital apparatus complies with Canadian ICES-003.

Europe – CE This digital equipment fulfills the requirements for radiated emission according to limit B of EN55022/1998, and the requirements for immunity according to EN55024/1998 residential, commercial, and industry.

Japan – This is a class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Australia – This electronic device meets the requirements of the Radio communications (Electromagnetic Compatibility) Standard AS/NZS CISPR22.

Liability

Every care has been taken in the preparation of this manual. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Trademark Acknowledgments

Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, OS/2, UNIX, Wfine, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc. UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:
- download user documentation and firmware updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrases
- report problems to Axis support by logging in to your private support area
- visit Axis Support at www.axis.com/techsup/

Safety Notice - Battery Replacement

The AXIS 221 uses a 3.0V CR2032 Lithium battery as the power supply for its internal real-time clock (RTC). Under normal conditions this battery will last for a minimum of 5 years. Low battery power affects the operation of the RTC, causing it to reset at every power-up. A log message will appear when the battery needs replacing.

The battery should not be replaced unless required!
If the battery does need replacing, please observe the following:
- Danger of Explosion if battery is incorrectly replaced
- Replace only with the same or equivalent battery, as recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions

AXIS 221 User's Manual
Revision 3.0
Part No: 29833
September 2007
Copyright© Axis Communications AB, 2005- 2007

Contents

Product Features 5
Overview 6
Accessing the Camera 8
Access from a browser 8
Setting the root password 9
Accessing the camera from the Internet 9
Focusing 9
The Live View page 10
Video Streams 12
Video stream types 12
MPEG-4 protocols and communication methods 13
How to stream MPEG-4 13
The AXIS Media Control 14
Other methods of accessing the video stream 14
Setup Tools 16
Accessing the setup tools from a browser 16
Video and Image Settings 17
Image Settings 17
Overlay/Mask Settings 18
Advanced settings 20
Live View Config 23
HTML Examples 26
External Video 26
Sequence Mode 26
Event Configuration 27
Event Servers 27
Configuring Event Types 28
Camera Tampering 30
Motion Detection 31
Port Status 32
System Options 33
Security - Users 33
Security - 802.1x 35
Date & Time 37
Network - Basic TCP/IP Settings 37

Network - Advanced TCP/IP Settings 38
Network - SOCKS 40
Network - QoS (Quality of Service) 41
Network - SMTP (email) 41
Network - SNMP 42
Network - UPnP™ 42
Network - RTP (Multicast)/MPEG-4 42
Network - Bonjour 42
Ports & Devices 42
LED Settings 43
Maintenance 43
Support 43
Advanced 44
About 45
Resetting to the Factory Default Settings 45
Unit Connectors 46
I/O Terminal connector 46
Power connections 48
The RS-232 connector 49
Troubleshooting 50
Checking the Firmware 50
Upgrading the Firmware 50
Emergency Recovery Procedure 51
Replacing the lens 55
Removing and attaching the lens 55
Technical Specifications 56
General performance considerations 59
Optimizing your system 59
Frame rates - Motion JPEG and MPEG-4 60
Bandwidth 60
Glossary of Terms 61
Index 63

Product Features

The AXIS 221 is part of the latest generation of fully featured Axis Network Cameras, based on the AXIS ARTPEC-2 compression chip. It features a DC-Iris and supports Power over Ethernet. It also features a metal casing and an infrared (IR) filter for day and night operation.

Video from the camera is made available on the network as a real-time, full frame rate Motion JPEG stream and/or MPEG-4 video stream. The camera includes **Video Motion Detection**, which can be used to trigger e.g. image uploads when there is activity in the video image. Uploads can also be scheduled to run at specified times. Security features include IP address filtering, encrypted browsing with HTTPS and multilevel password protection.

The AXIS 221 is equipped with two alarm inputs and one output, which can be connected to various external devices, e.g. door sensors and alarm bells.

Video can be viewed in various different resolutions. Up to 20 viewers can access the AXIS 221 simultaneously when using Motion JPEG and MPEG-4 unicast. The number of simultaneous viewers can be increased by using multicast MPEG-4.

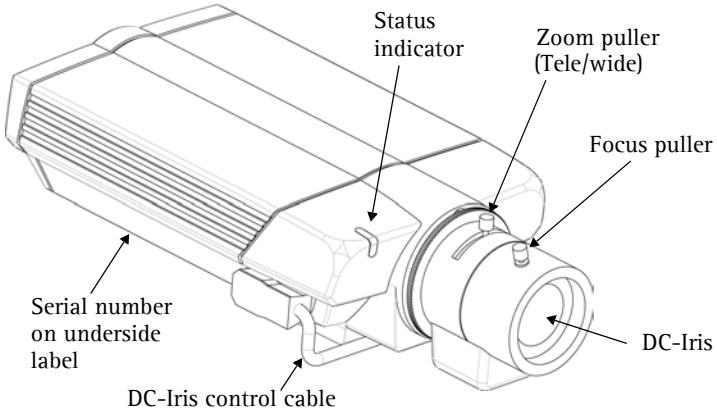
Each MPEG-4 viewer requires a separate MPEG-4 decoder license, of which one is included. Additional licenses can be purchased separately from your Axis dealer. If using other clients to view the MPEG-4 video stream, no further MPEG-4 decoder licenses are required.

The camera has a built-in Web server, providing full access to all features through the use of a standard web browser. The built-in scripting tool allows the creation of basic applications. For advanced functionality, the camera can be accessed via the AXIS HTTP API (more info at www.axis.com/developer).

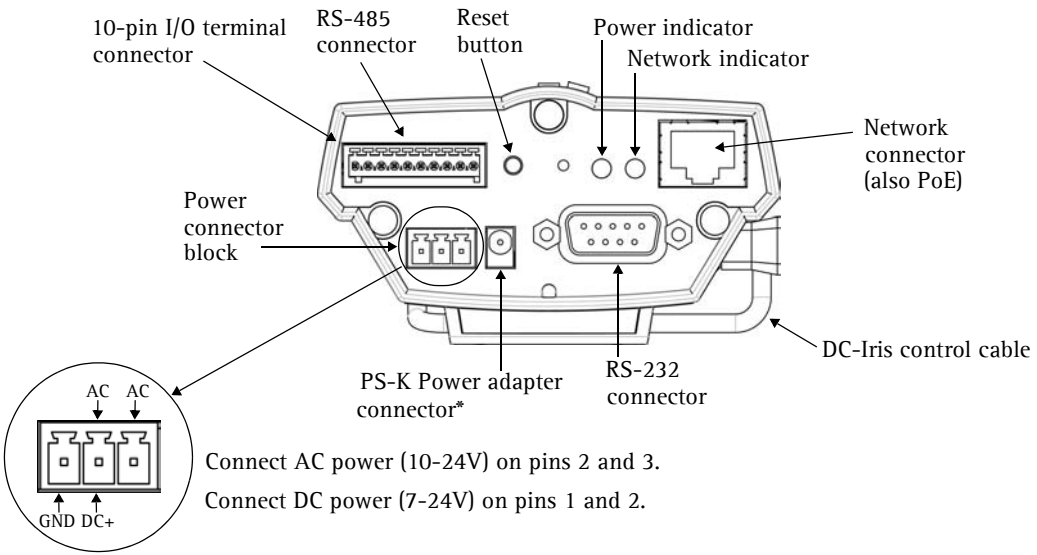
The AXIS 221 features a varifocal lens with DC-Iris, which automatically regulates the amount of light entering the camera. Tele/wide and focus are adjusted manually with the aid of the pullers mounted on the lens. The AXIS 221 is also available without a lens.

The AXIS 221 can be powered from the network cabling and supports Power over Ethernet (PoE) network transformers conforming to IEEE 802.3af.

Overview



Rear panel



*only use the supplied PS-K power adapter

Power adapter connector - for connection of the PS-K power adapter (included).

Power connector block - for connection of a power supply. See *Power connections,* on page 48 .

I/O terminal connector - The I/O terminal connector provides the physical interface to one solid state relay output, two digital photo-coupled inputs, RS-485 and an auxiliary connection point for DC power. For more information, see *Unit Connectors*, on page 46.

Network connector - The AXIS 221 connects to the network via a standard network cable, and automatically detects the speed of the local network segment (10BaseT/100BaseTX Ethernet). This socket can also be used to power the AXIS 221 via PoE (Power over Ethernet). The camera also negotiates the correct power level when using PoE.

RS-232 connector - Single 9-pin D-SUB RS-232 connector, max 115 kbit/s, half-duplex.

Serial number - This number is used during installation.

Reset button - Press this button to install the AXIS 221 using the AXIS Internet Dynamic DNS Service (see the installation guide), or to restore the camera to its factory default settings, as described in *Resetting to the Factory Default Settings,* on page 45.

LED indicators

After completion of the startup and self test routines, the multi-colored Network, Status, and Power LED indicators flash as follows:

Network	Amber	Steady for connection to 10 Mbit/s network. Flashes for network activity.
	Green	Steady for connection to 100 Mbit/s network. Flashes for network activity.
	Unlit	No connection.
Status	Green	Shows steady green for normal operation. Can be configured to flash green at intervals whenever the camera is accessed. See the online help for more information.
	Amber	Shows steady amber during reset to factory default or when restoring settings.
	Red	Slow flash for failed firmware upgrade (see *Emergency Recovery Procedure*, on page 51).
	Unlit	When configured for "no flash" on camera access.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.

Accessing the Camera

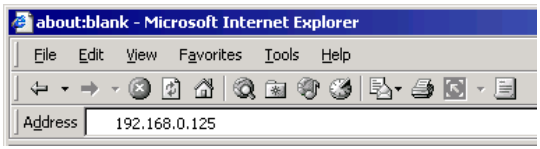
Follow the instructions in the AXIS 221 Installation Guide to install the camera.

The camera can be accessed with most standard operating systems and browsers. The recommended browser is Internet Explorer for Windows, and Mozilla with other operating systems. See also the *Technical Specifications,* on page 56.

Note: To view streaming video in Microsoft Internet Explorer, you must set your browser to allow the AXIS Media Control (AMC) to be installed on your computer. The first time an MPEG-4 video stream is accessed AMC also installs an MPEG-4 decoder for viewing the video streams. As a license is required for each instance of the decoder, the product administrator may have disabled the installation. See page 21 for more information. If your workstation restricts the use of additional software components, the camera can be configured to use a Java applet for updating JPEG images. See the online help for more information.

Access from a browser

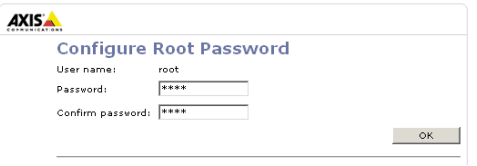
1. Start a browser (e.g. Internet Explorer, Mozilla)
2. Enter the IP address or host name of the camera in the **Location/Address** field of your browser.



3. If this is the first time the camera is accessed, see *Setting the root password,* on page 9. Otherwise enter your user name and password, as set by the administrator.
4. The camera's **Live View** page is now displayed in your browser.

Note: The layout of the live view page in the camera may have been customized to meet specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own Live View page.

Setting the root password



1. When accessing the camera for the first time, the '**Configure Root Password**' dialog will be displayed on the screen.
2. Enter a password and then re-enter it, to confirm the spelling. Click **OK**.
3. The **Enter Network Password** dialog will appear. Enter the User name: **root** **Note:** The default administrator user name **root** is permanent and cannot be deleted or altered.
4. Enter the password as set in step 2 above, and click **OK**. If the password is lost, the camera must be reset to the factory default settings. See page 45.
5. If required, click **Yes** to install the AXIS Media Control (AMC). You will need administrator rights on the computer to do this.

Accessing the camera from the Internet

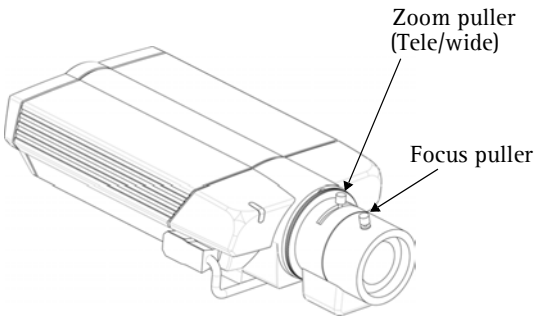
Once installed, the camera is accessible on your local network (LAN). To access the camera from the Internet you must configure your router/firewall to allow incoming data traffic. For security reasons this is usually done on a specific port. Please refer to the documentation for your router/firewall for further instructions.

For more information, please visit the AXIS Internet Dynamic DNS Service at www.axiscam.net or, for Technical notes on this and other topics, visit the Axis Support Web at www.axis.com/techsup

Focusing

To focus the AXIS 221, follow the instructions below.

1. From the **Basic Configuration** page in the setup tools, open the **Focus adjustment** page.
2. Set the DC-Iris to *Disabled* and click **Save**.
3. Unscrew the zoom puller on the lens by turning it anti-clockwise. Adjust the zoom setting as required. Re-tighten the zoom puller.
4. Unscrew the focus puller on the lens. Adjust the focus as required. Re-tighten the focus puller.

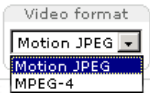


5. From the Focus adjustment page, set the DC-Iris to *Enabled* and click **Save**.

Note: The DC-Iris should always be disabled while focusing the camera. This opens the iris to its maximum, which gives the smallest depth of field and thus the best conditions for correct focusing. When the focus is set with this method it will then be maintained in any light conditions.

The Live View page

Depending on whether or not the Live View page has been customized, the buttons described below may or may not be visible.



The Video Format drop-down list allows the video format on the Live View page to be temporarily changed.

The **Output buttons**, **Pulse** and **Active/Inactive** below, control the output directly from the **Live View** page. These buttons are configured under **Setup > Live View Config > Layout**.

Pulse - click this button to activate the output for a defined period of time, e.g. to switch on a light for 20 seconds.

Active/Inactive - click these buttons to manually start and stop a connected device, e.g. switch a light on/off.

These buttons start and stop the **Sequence Mode**. This mode is created in **Setup > Live View Config > Sequence mode**, and automatically displays the view from 2 or more video sources at set intervals.

From the **Source** list, select the desired external video source. Note that Sequence Mode must be stopped before selecting a source from this list.

The **Trigger buttons** can trigger an event directly from the **Live View** page. These are configured under **Setup > Live View Config > Layout**.

The **Snapshot** button saves a snapshot of the image currently being displayed. Right-click on the video image to save it in JPEG format on your computer. This button is intended for use when the AMC viewer toolbar is not available.

The AMC (AXIS Media Control) **viewer toolbar** is available in **Microsoft Internet Explorer only.** It displays the following buttons:

Play/Stop buttons - start and stops the live video stream.

The **Snapshot** button saves a snapshot of the video image currently being displayed. The Snapshot function and the target directory for saving snapshots can be configured from the AMC Control Applet in the Windows Control Panel (Internet Explorer only).

The record button is used to record the current (MPEG-4) video stream. The location where the image file is saved can be specified using the AMC control panel. To enable recording, Select **Live View Config > Viewer Settings > Enable recording button**.

Click the **View Full Screen** button to make the video image fill the entire screen area. No other windows will be visible. Press **Esc** (Escape) on the computer keyboard to exit full screen.

Video Streams

The AXIS 221 provides several different image and video formats. The type to use depends on your requirements and on the properties of your network.

The Live View page in the AXIS 221 provides access to Motion JPEG and MPEG-4 video streams, as well as to single JPEG images. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

Video stream types

Motion JPEG

This format uses standard JPEG still images in the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but also provides excellent image quality and access to each and every individual image contained in the stream.

Note also that multiple clients accessing Motion JPEG streams can use different image settings.

MPEG-4

This is a video compression standard that makes good use of bandwidth, and which can provide high-quality video streams at less than 1 Mbit/s.

The MPEG-4 standard provides scope for a large range of different coding tools for use by various applications in different situations, and the AXIS 221 provides certain subsets of these tools. These are represented as **Video object types**, which are selected for use with different viewing clients. The supported video object types are:

- **Simple** - sets the coding type to H.263, as used by e.g. QuickTime™.
- **Advanced Simple** - sets the coding type to MPEG-4 Part 2, as used by AMC (AXIS Media Control)

When using MPEG-4 it is also possible to control the bit rate, which in turn allows the amount of bandwidth usage to be controlled. CBR (Constant Bit Rate) is used to achieve a specific bit rate by varying the quality of the MPEG-4 stream. When using VBR (Variable Bit Rate), the quality of the video stream is kept as constant as possible, at the cost of a varying bit rate.

Notes:
- MPEG-4 is licensed technology. The AXIS 221includes one viewing client license. Installing additional unlicensed copies of the viewing client is prohibited. To purchase additional licenses, contact your Axis reseller.
- All clients viewing the MPEG-4 stream must use the same set of coding tools.

MPEG-4 protocols and communication methods

To deliver live streaming video over IP networks, various combinations of transport protocols and broadcast methods are employed.

- RTP (Realtime Transport Protocol) is a protocol that allows programs to manage the real-time transmission of multimedia data, via unicast or multicast.
- RTSP (Real Time Streaming Protocol) serves as a control protocol, to negotiate which transport protocol to use for the stream. RTSP is thus used by a viewing client to start a unicast session, see below.
- UDP (User Datagram Protocol) is a communications protocol that offers limited service for exchanging data in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). The advantage of UDP is that it is not required to deliver all data and may drop network packets when there is e.g. network congestion. This is suitable for live video, as there is no point in re-transmitting old information that will not be displayed anyway.
- Unicasting is communication between a single sender and a single receiver over a network. This means that the video stream goes independently to each user, and each user gets their own stream. A benefit of unicasting is that if one stream fails, it only affects one user.
- Multicast is bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients. This technology is used primarily on delimited networks (intranets), as each user needs an uninterrupted data flow and should not rely on network routers.

How to stream MPEG-4

Deciding on the combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. Setting the preferred method(s) is done in the control applet for AMC, which is found in the Windows Control Panel. When this has been set, AMC will test all the selected methods in the specified order, until the first functioning one is found.

RTP+RTSP

This method (actually RTP over UDP and RTSP over TCP) should be your first consideration for live video, especially when it is important to always have an up-to-date video stream, even if some images are lost due to network problems. This can be configured as multicast or unicast.

Multicasting provides the most efficient usage of bandwidth, especially when there are large numbers of clients viewing simultaneously. Note however, that a multicast broadcast cannot pass a network router unless the router is configured to allow this. It is thus not possible to multicast over e.g. the Internet.

Unicasting should be used for video-on-demand broadcasting, so that there is no video traffic on the network until a client connects and requests the stream. However, as more and more unicast clients connect, the traffic on the network will increase and may cause congestion. Although there is a maximum of 20 unicast viewers, note that all multicast users combined count as 1 unicast viewer.

RTP/RTSP

This unicast method is RTP tunneled over RTSP. This can be used to exploit the fact that it is relatively simple to configure firewalls to allow RTSP traffic.

RTP/RTSP/HTTP or RTP/RTSP/HTTPS

These two methods can also be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.

The AXIS Media Control

The recommended method of accessing live video (MPEG-4 and/or Motion JPEG) from the AXIS 221 is to use the AXIS Media Control (AMC) in Microsoft Internet Explorer for Windows. This ActiveX component is automatically installed on first use, after which it can be configured by opening the AMC Control Panel applet from the Windows Control Panel. Alternatively, right-click the video image in Internet Explorer.

Other methods of accessing the video stream

Video/images from the AXIS 221 can also be accessed in the following ways:

- If supported by the client, the AXIS 221 can use Motion JPEG server push to display video. This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- As single JPEG images in a browser. Enter e.g. the path: http://<IP address>/axis-cgi/jpg/image.cgi?resolution=320x240
- Windows Media Player. This requires AMC and the MPEG-4 decoder to be installed. The paths that can be used are listed below in the order of preference.
    - Unicast via RTP: axrtpu://<IP address>/mpeg4/media.amp
    - Unicast via RTSP: axrtsp://<IP address>/mpeg4/media.amp
    - Unicast via RTSP, tunneled via HTTP: axrtsphttp://<IP address>/mpeg4/media.amp
    - Unicast via RTSP, tunneled via HTTPS: axrtsphttps://<IP address>/mpeg4/media.amp
    - Multicast: axrtpm://<IP address>/mpeg4/media.amp

Other MPEG-4 clients

Although it may be possible to use other clients to view the MPEG-4 stream, this is not guaranteed by Axis.

For some other clients, e.g. QuickTime™ the Video Object Type must be set to *Simple*. It may also be necessary to adjust the advanced MPEG-4 settings.

To assess the video stream from e.g. QuickTime™ the following path can be used:

rtsp://<IP address>/mpeg4/media.amp

This path is for all supported methods, and the client will negotiate with the AXIS 221 to determine exactly which transport protocol to use.

Setup Tools

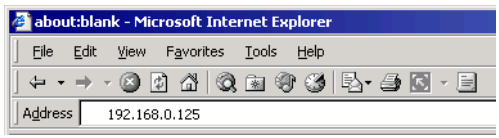
The AXIS 221 is configured from the setup tools, which are available from the link in the web interface. The setup tools can be used by:

- **Administrators**, who have unrestricted access to all the Setup tools
- **Operators**, who have access to the Video & Image, Live View Config and Event Configuration settings.

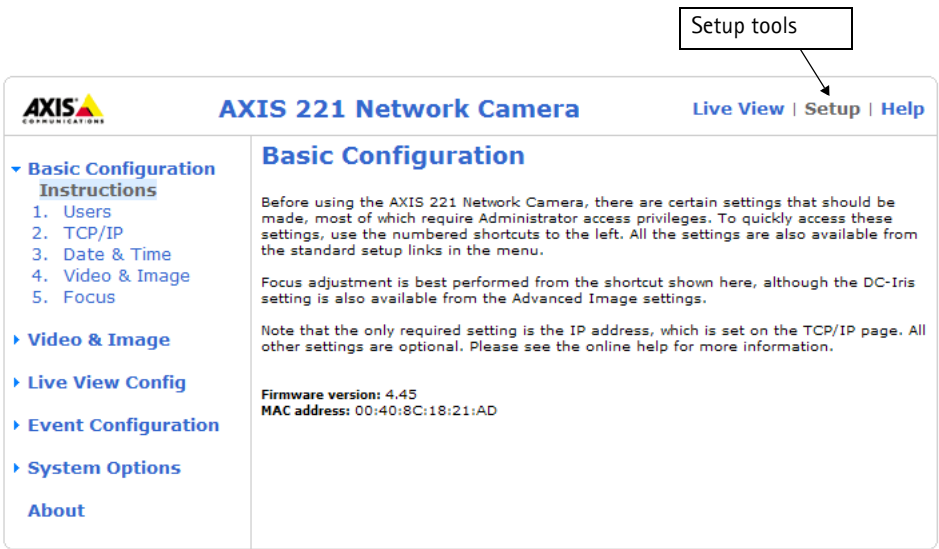
Accessing the setup tools from a browser

Follow the instructions below to access the Setup Tools from a browser.

1. Start your browser and enter the IP address or host name of the camera in the location/address field.



2. The **Live View** page is now displayed. Click **Setup** to display the **Setup** tools.


Setup tools
AXIS 221 Network Camera
Live View | Setup | Help
Basic Configuration
Instructions
1. Users
2. TCP/IP
3. Date & Time
4. Video & Image
5. Focus
Video & Image
Live View Config
Event Configuration
System Options
About
Basic Configuration
Before using the AXIS 221 Network Camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the numbered shortcuts to the left. All the settings are also available from the standard setup links in the menu.
Focus adjustment is best performed from the shortcut shown here, although the DC-Iris setting is also available from the Advanced Image settings.
Note that the only required setting is the IP address, which is set on the TCP/IP page. All other settings are optional. Please see the online help for more information.
Firmware version: 4.45
MAC address: 00:40:8C:18:21:AD

Video and Image Settings

The following descriptions show examples of some of the features available in the AXIS 221. For details of each setting, please refer to the online help available from the setup tools. Click to access the online help.

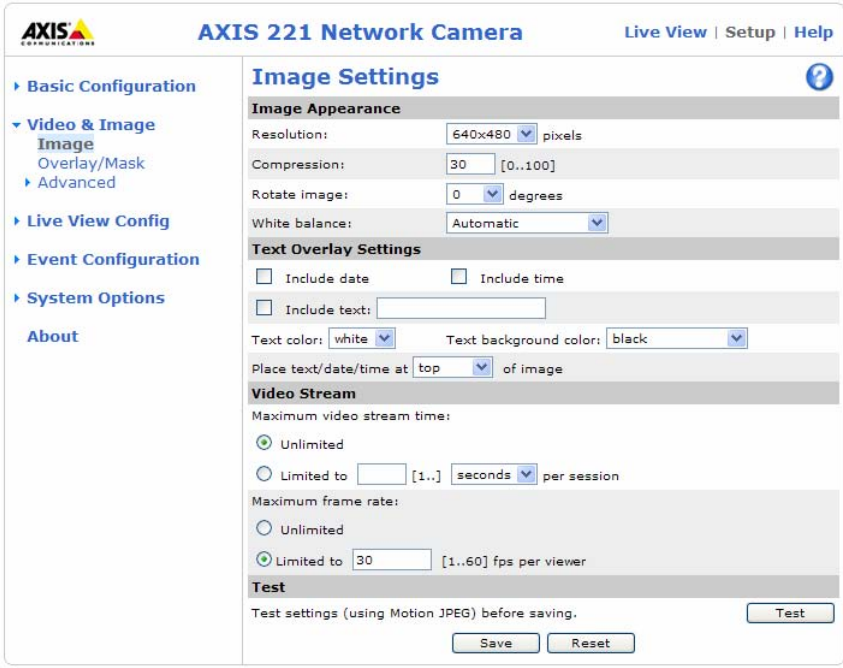


Image Settings

Image Appearance

Adjust these settings to optimize the video images according to your requirements.

All configuration of images and overlays will affect the camera's overall performance, depending on how it is used and on the available bandwidth. Lower compression improves video image quality, but increases the bandwidth.

Changed video image settings have immediate effect on the MPEG-4 stream, but the Motion JPEG stream will have to be started (or restarted) before the settings take effect.

Text Overlay Settings

The date, time, and user defined text can be included on one line, either on the top or bottom of the video image.

It is also possible to set how the text and text background are displayed. You can set the text to be either black or white, and the text background can also be set to black, white, semi-transparent, or transparent.

Please see the online help for further information on these settings.

Video Stream

Define the maximum **video stream time** per session in seconds, minutes or hours. When the set time has expired, a new stream can be started by refreshing the page in the Web browser. For unlimited video stream time, set this value to 0. This setting is only applicable to Motion JPEG.

The **frame rate** allowed to each viewer can also be limited, to avoid bandwidth problems on the network.

Test

To preview the image before saving, click **Test**. Note that the preview image will be in JPEG format, even though the settings are valid both for Motion JPEG and MPEG-4.

Overlay/Mask Settings

Overlay/Mask Type

When using an image overlay, select from the following options the type to use:

- Uploaded image as overlay - usually used to provide extra information in the video image.
- Uploaded image as privacy mask - conceals part of the video image.
- Configurable areas as privacy masks - up to 3 black areas are used to conceal parts of the video image.

The difference between an overlay and a privacy mask is that a privacy mask cannot be bypassed by accessing the video stream with the help of the AXIS HTTP API, whereas an overlay can.

Selecting the overlay/mask type will display further settings available for the selected type. See the online help for further information.

Upload and use an overlay

To upload an overlay image to the camera:

1. Select the type of overlay to use in **Overlay/Mask Type**.
2. In the field **Upload own image**, click the **Browse** button and locate the image file on your computer or server.
3. Click the **Upload** button and follow the on-screen instructions.

To use an already uploaded image:

1. Select an uploaded image from the **Use image** drop-down list.
2. Place the image at the required location by entering the x and y coordinates.
3. Click **Save.**

Overlay image requirements

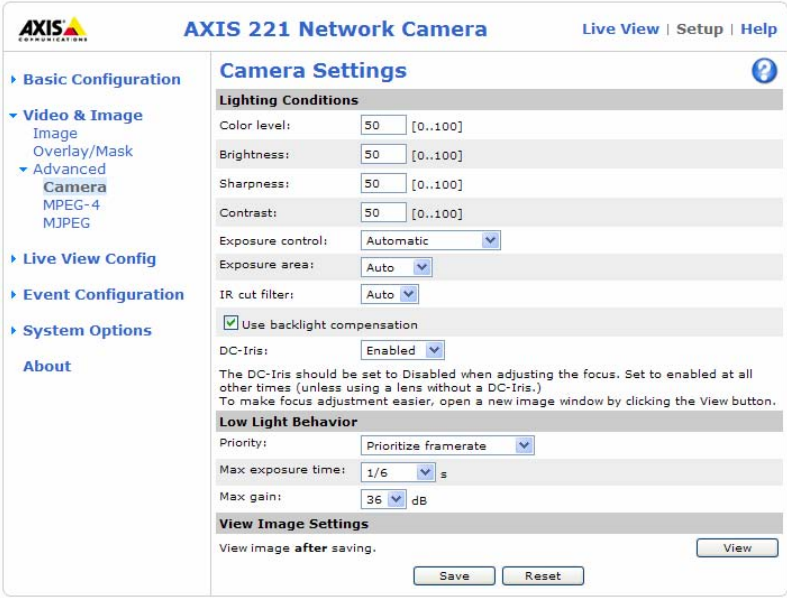
Image Formats	Image Size
• Windows 24-bit BMP (full color) • Windows 4-bit BMP (16 colors)	The height and width of the overlay image in pixels must be exactly divisible by 4.

There are a number of limitations when using overlay images, such as the size and positioning of images. Please refer to the online help for more information.

Advanced settings

These web pages include different settings for fine-tuning the video image.

Camera settings



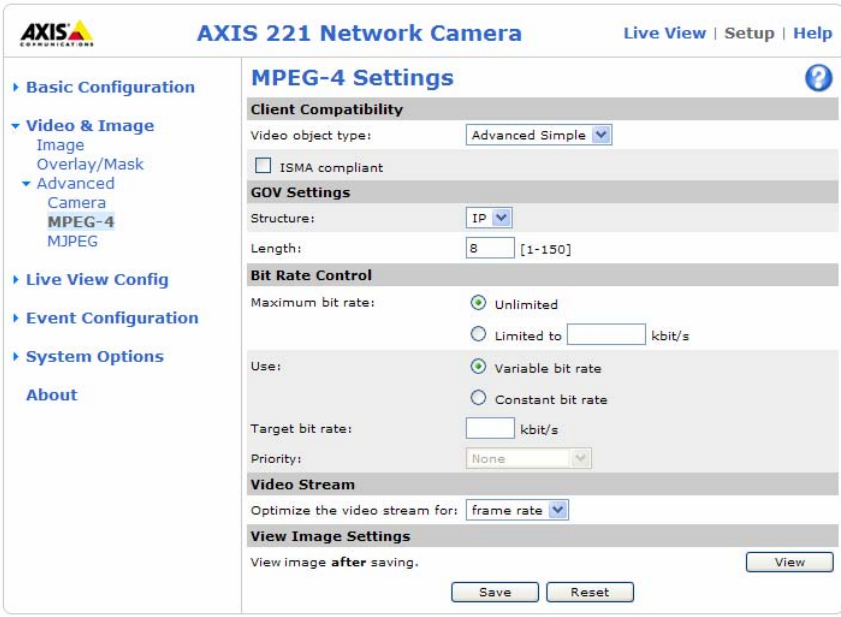
To compensate for the **Lighting Conditions**, the **Color level**, the **Brightness**, the **Sharpness**, the **Contrast**, and the **Exposure control**, the **Exposure area** and the **IR cut filter** can all be adjusted. **DC-Iris** should always be enabled, except when focusing, or when using a non-DC-Iris lens.

The settings for **Low Light Behavior** determine how the camera will behave at low light levels. These settings all affect video image quality and are basically a measure of how much noise to allow in the video images.

Please see the online help for further information on these settings.

MPEG-4 Settings

These are the tools for adjusting the MPEG-4 settings and controlling the video bit rate.



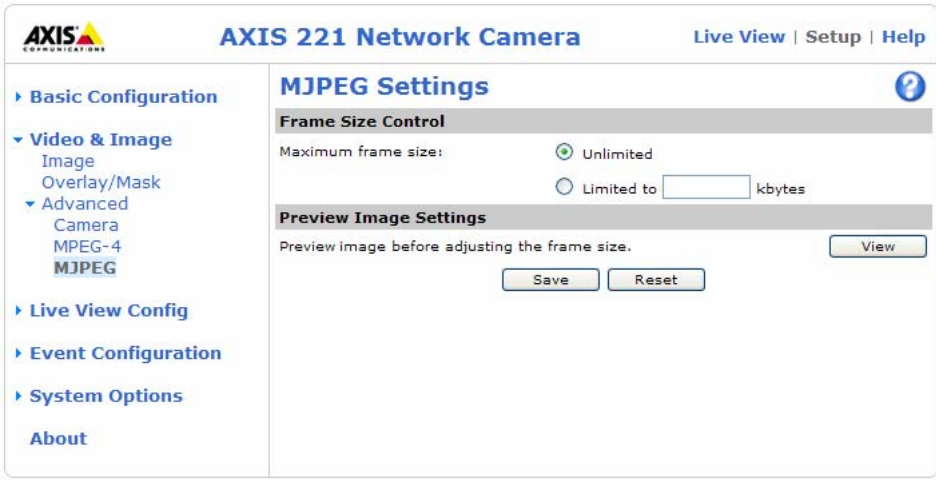
The MPEG-4 standard provides many different coding tools for various applications in different situations. As most MPEG-4 clients do not support all of these tools, it is usual to instead define and use subsets for different clients or groups of clients. These settings allow you to define the type of viewing client to use.

Adjusting the maximum bit rate and setting it to variable or constant is a good way of controlling the bandwidth used by the MPEG-4 video stream.

For more information on these advanced settings, please see the online help, and *Video stream types*, on page 12.MJPEG Settings

MJPEG Settings

The MJPEG Settings window is used to control the frame size of the video stream in order to improve either image quality or save bandwidth.



Frame Size Control - Use **Frame Size Control** to set the maximum frame size to unlimited for best image quality, or to a limited number of Kbytes. The default is set to unlimited.

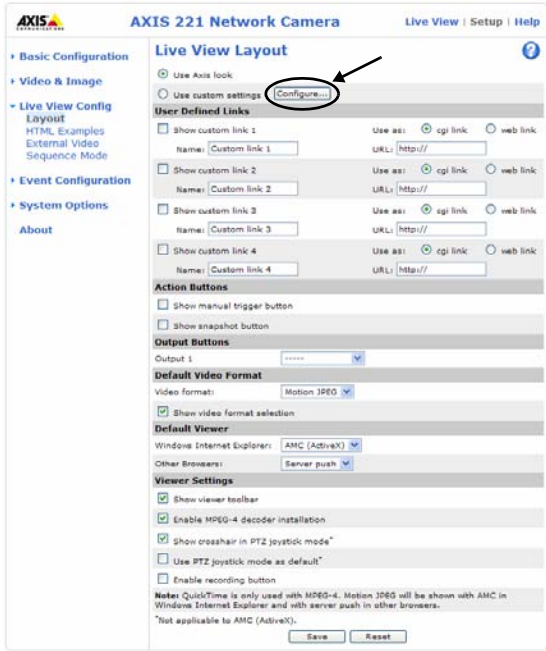
Preview Image Settings - Use **Preview Image Settings** to view the current compression and frame size settings in the text overlay at the top of the image.

Live View Config

These are the tools for deciding the layout of the camera's Live View page. The layout can be set in 3 ways:

- **Use Axis look** - the layout is unchanged.
- **Use custom settings** - modify the default Live View page with your own colors, images etc. Click the **Configure** button and see below.
- **Own Home Page** - Use your own custom page as the default web page. Click the **Configure** button and see the following page.

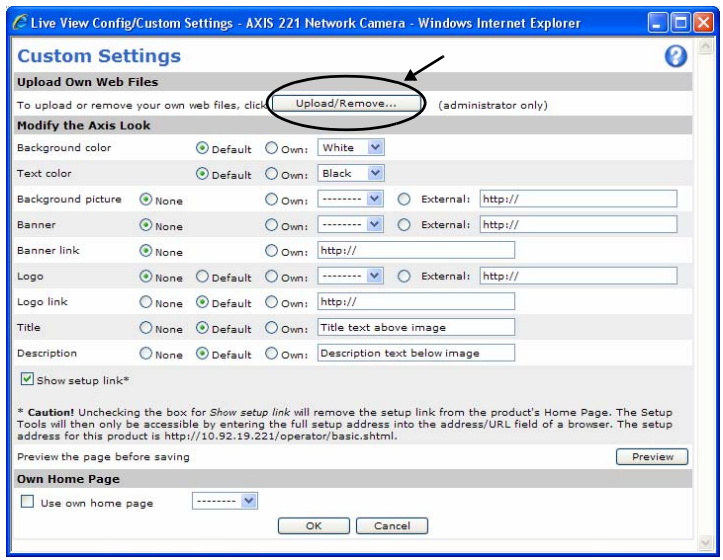
The other settings on this page concern which other features to include, e.g. buttons and links. See page 24 for more information.



Use custom settings

Adjust the settings under **Modify the Axis look**, to change the background picture, banner, colors, etc.

To use your own file for e.g. a banner, first upload it (see the following page) or select **External** and enter the path to the file.



Note that unchecking the box for **Show setup link** will remove the setup link from the camera's Home Page. The setup tools will then only be accessible by entering the full setup address into the address/URL field of a browser, i.e.

http://<ip address>/operator/basic.shtml

Upload Own Web Files

Your own background pictures, banners and logos can either be located externally on e.g. a network server, or they can be uploaded to the AXIS 221 itself. Once uploaded, files are shown in the drop-down lists for **Own** (file). Follow these instructions to upload a file.

1. Click the **Upload/Remove** button in the Custom settings dialog.
2. Enter the path to the file, e.g. a file located on your computer or click the **Browse** button.
3. Select the user level for the uploaded file. Setting the user access level means that you have complete control over which pages can be viewed by which users.
4. When the path is shown correctly in the text field, click the **Upload** button.

All uploaded files are shown in the list in the lower section of this dialog. To remove a file, check the box provided next to it and then click the **Remove** button.

Own home page

From Live View Layout, select the radio button **Use custom settings** and click **Configure**.

Check the box **Use own home page** at the bottom of this dialog, To use a previously uploaded web page (see above) as the default home page, select the page from the drop-down list and click OK.

User-defined Links

Enter a descriptive name and enter the URL in the provided field.

Example

1. Check **Show custom link 1**
2. Enter a descriptive name, e.g. My Website
3. Check the radio button for **web link**
4. Enter the web link: e.g. http://www.example.com
5. Click **Save**.

This link will then be shown on the Live View page and will open the specified web site.

User-defined CGI links can be used to issue advanced commands via the Axis HTTP API. For more information, see the Developer pages at www.axis.com/developer

Action Buttons

The **manual trigger** buttons can be used to manually trigger and stop an event from the Live View page. See *Event Configuration,* on page 27.

Enabling the display of the **Snapshot** button allows users to save a snapshot from the video stream by clicking this button. This button is mainly intended for use with browsers other than Internet Explorer for Windows, or when otherwise not using ActiveX to view the video stream. The ActiveX viewing component (AXIS Media Control) for Internet Explorer provides its own snapshot button.

Output Buttons

These buttons can then be used to manually activate the output from the Live View page, e.g. to switch a light on and off. There are 2 options for how the output is activated:

- The Pulse button activates the output for a defined period
- Active/Inactive displays 2 buttons, one for each action (on/off)

Default Video Format

Select default video format from the drop-down list. Checking the box for **Show video format selection** displays a drop-down list on the Live View page allowing you to temporarily change the format.

Default Viewer

When using *Microsoft Internet Explorer (IE)* for Windows, select your preferred method of viewing moving images. The options are:

- **AMC(ActiveX)**- This is the best choice for fast image updating in Internet Explorer, but might not be possible on computers that have restriction on the installation of additional software.
- **QuickTime** - For use with MPEG-4 only, select this to use the QuickTIme plug-in for Microsoft Internet Explorer.
- **Java applet** - This alternative uses a Java applet to update the images in the browser.
- **Still Image** - Displays still images only. Hit the **Refresh** button in your browser to view a new image.

When using any other browser than Internet Explorer for Windows, select the appropriate method from the drop-down list for viewing images. The available options are similar to Internet Explorer except for **Server Push.** With this method, the camera maintains and controls an open HTTP connection to the browser and sends data as and when required for as long as required. Please see the online help for more information.

Viewer settings

Checking the **Show viewer toolbar** displays the viewer toolbar under the video stream in your browser. By checking the **Enable MPEG-4 decoder installation** box, it is also possible for the Administrator to enable or disable the installation of the MPEG-4 decoder. This is used to prevent the installation of unlicensed copies. Further decoder licenses can be purchased from your Axis dealer.

HTML Examples

You can add live video from the camera to your own web site. The camera can transmit a Motion JPEG or unicast MPEG-4 stream to up to 20 simultaneous connections, although an administrator can restrict this to fewer. If multicast MPEG-4 is used, the video stream will be available to an unlimited number of viewers connected to the parts of the network where multicast is enabled. Please note that a separate MPEG-4 license is required for each viewer.

Enter the **Video Format**, **Image Type**, **Image Size** and other settings to suit your Web page and click **Update**. The camera then generates the required source code for your configuration. Copy this code and paste it into your own Web page code.

External Video

The camera can also display video images from other Axis network cameras and video servers, directly on the Live View page. These are known as **External Video** sources. These external video sources are available from the drop-down list on the Live View page.

Click the **Add** button to open the External Video Source Setup dialog, which is used to make all the necessary settings. Enter the IP address or host name of the external video source you wish to add. Depending on the external source, then select either MPEG-2, MPEG-4 or Motion JPEG as the type of video stream to receive.

Example of a path to an external video source:

```
http://192.168.0.125/axis-cgi/mjpeg/video.cgi
```

Sequence Mode

The Live View page can be configured to cycle through the internal and selected external video sources, in order, or randomly.

Select the desired video sources and enter the time in seconds to display each source (up to 59 minutes). Click **Save**.

The Sequence buttons that appear on the Live View page are used to start and stop the sequence mode.

Please see the online help for more information.

Event Configuration

An **event** in the camera is when an **Event Type** is activated and causes certain actions to be performed. The event type is the set of parameters (or conditions) that specifies how and when which actions will be performed. A common event type is when the camera uploads images when an alarm occurs. Many event types use an **Event Server**, to e.g. upload images to.

This section describes how to set up event servers and event types, i.e. how to configure the camera to perform certain actions when events (e.g. alarms) occur.

Definitions

Event type	A set of parameters describing how and when the camera will perform certain actions
Triggered Event - see page 28	An event that is started by some sort of signal, e.g. from an external device, such as a door switch, motion detection, system event, etc.
Scheduled Event - see page 29	Pre-programmed time period(s) during which an event will run.
Action	That which occurs when the event runs, e.g. the upload of images to an FTP server, e-mail notification, etc.

Event Servers

Event Servers are used to receive e.g. uploaded image files and/or notification messages. To set up Event server connections in your camera, go to **Setup > Event Configuration > Event Servers** and enter the required information for the required server type.

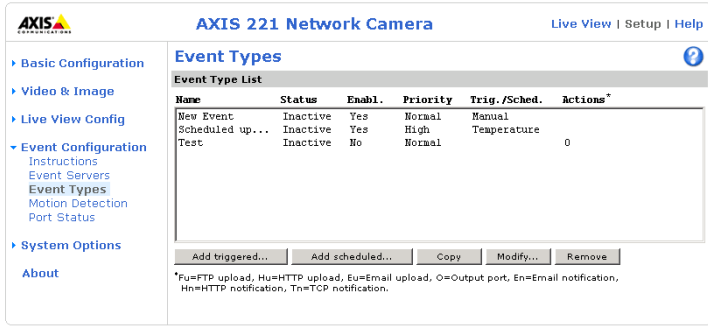
Server type	Purpose	Information required
FTP Server	• Receives uploaded images	• Descriptive name of your choice • Network address (IP address or host name) • User name and password (for FTP server)
HTTP Server	• Receives notification messages • Receives uploaded images	• Descriptive name of your choice • URL (IP address or host name) • User name and password (for HTTP server)
TCP Server	• Receives notification messages	• Descriptive name of your choice • Network address (IP address or host name) • Port number

For details on each setting, please see the online help available from each web page.

When the setup is complete, the connection can be tested by clicking the **Test** button (the connection test takes approximately 10 seconds).

Configuring Event Types

An **Event Type** describes how and when the camera will perform certain actions.



Example: If somebody passes in front of the camera, and an event that uses motion detection has been configured to act on this, the camera can e.g. record and save images to an FTP server, and/or send a notification e-mail to a pre-configured e-mail address with a pre-configured message. Images can be sent as e-mail attachments. See File Naming & Date/Time Formats under Event Configuration in the online help.

Triggered Event

A Triggered event can be activated by:

- a switch (e.g. a push button) connected to the camera's input port
- detected movement in a configured motion detection window
- a manually activated action, e.g. from an action button in the web interface
- on restart (reboot) after e.g. power loss
- a temperature warning
- a camera tampering alarm

How to set up a triggered event

This example describes how to set the camera to upload images when e.g the main door is opened:

1. Click **Add triggered...** on the **Event Types** page.
2. Enter a descriptive **name** for the event, e.g. Main door open.
3. Set the **priority** - High, Normal or Low (see the online help).
4. Set **min time interval between triggers** - The shortest possible interval is 1 second and the longest is 23 hours, 59 minutes and 59 seconds. (see the online help).
5. Set the **Respond to Trigger...** parameters for when the event will be active, e.g. only after office hours.
6. Select the trigger alternative from the **Triggered by...** drop-down list, e.g. select Input ports, for the sensor connected to the door.
7. Set the **When Triggered...** parameters, i.e. define what the camera will do if the main door is opened e.g., upload images to an FTP server or send an e-mail.
8. Click **OK** to save the Event in the Event Types list.

Please use the online help for descriptions of each available option. Image file names can be formatted according to specific requirements, such as time/date or type of triggered event. See *File Naming & Date/Time Formats* under *Event Configuration*.

Note: Up to 10 event types can be configured in the camera, and up to 3 of these can be configured to upload images.

Pre-trigger and Post-trigger buffers

This function is very useful when checking to see what happened immediately before and/or after a trigger, e.g. up to 30 seconds before and/or after a door was opened. Check the **Upload images** checkbox under **Event Types > Add Triggered... > Triggered by...** to expand the web page with the available options. All uploaded images are JPEG images.

Include pre-trigger buffer - images stored internally in the camera from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer, enter the desired length of time and specify the required image frequency.

Include post-trigger buffer - contains images from the time immediately after the trigger. Configure as for pre-trigger.

Notes:
- Pre-trigger and Post-trigger buffers will be lost if the connection to the event server fails.
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate.
- If the pre- or post-buffer is too large for the camera's internal memory, the frame rate will be reduced and individual images may be missing. If this occurs, an entry will be created in the unit's log file.

Continue image upload (unbuffered) - enables the upload of video images for a fixed length of time. Specify the length of time for the uploaded recording, in seconds, minutes or hours, or for as long as the trigger is active. Finally, set the desired image frequency to the maximum (the maximum available) or to a specified frame rate. The frame rate will be the best possible, but might not be as high as specified, especially if uploading via a slow connection.

Scheduled Event

A **Scheduled event** can be activated at preset times, in a repeating pattern on selected weekdays.

Configuration example:

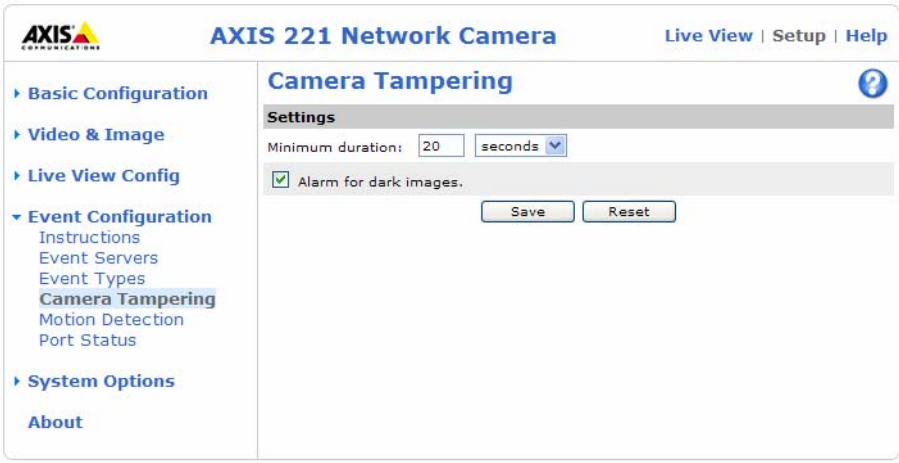
1. Click **Add scheduled...** on the **Event Types** page.
2. Enter a descriptive **name** for the event, e.g. “Scheduled e-mail upload.”
3. Set the **priority** (High, Normal or Low).
4. Set the **Activation Time** parameters (24h clock) when the event will be active, e.g. start on Sundays at 13.00 with a duration of 12 hours.
5. Set the **When Activated...** parameters, i.e. set what the camera will do at the specified time, e.g. send uploaded images to an e-mail address.
6. Click **OK** to save the Event in the Event Types list.

Please see the online help for descriptions of each available option.

Camera Tampering

The camera tampering application generates an alarm whenever the camera is repositioned, or when the lens is covered, sprayed, or severely defocused.

You must also create an event, see *How to set up a triggered event,* on page 28, for the camera to send an alarm.



Settings

Minimum duration - This parameter sets the minimum tampering period, i.e. an alarm will not be triggered until this period has elapsed, even if the tampering conditions are otherwise met. This can help prevent false alarms for known conditions that affect the image.

Alarm for dark images - If the camera lens is sprayed or covered so that the camera live view becomes dark, it will not be possible to distinguish this situation from other situations where the same effect is seen, i.e., when lighting conditions change.

When this paramater is enabled, alarms will be generated for all cases where the lights are either dimmed or turned off, or if the lens is sprayed, covered, or severely defocused. If not enabled, no alarm will be sent.

After making these settings, click **Save**.

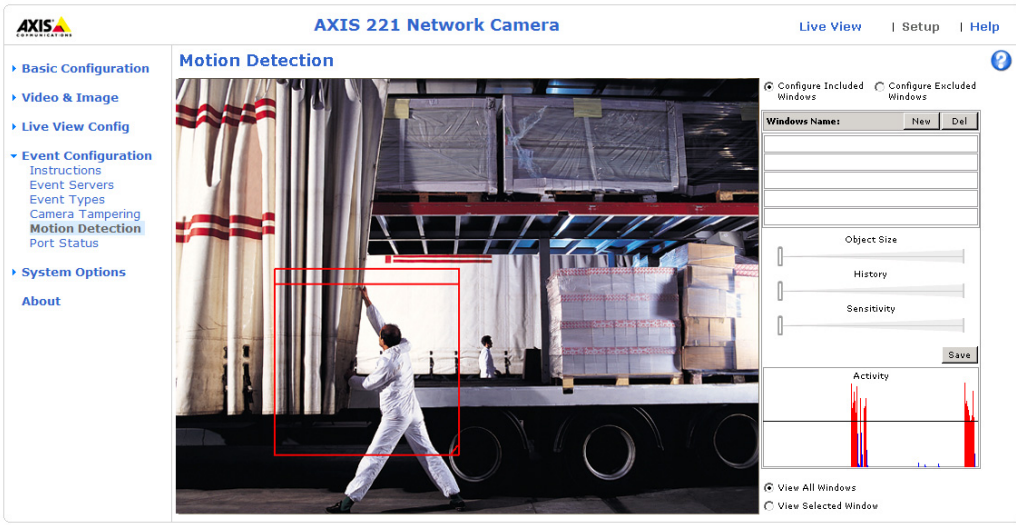
Motion Detection

Motion detection is used to generate an alarm whenever movement either occurs or stops in the video image. A total of 10 Include and/or Exclude windows can be configured.

- **Included** windows target specific areas within the whole video image
- **Excluded** windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

Once configured, the motion detection windows will appear in the list of available triggers, for triggering events. See *How to set up a triggered event* above.

Note: Using the motion detection feature may decrease the camera's overall performance.



Configuring Motion Detection

1. Click **Motion Detection** in the **Event Configuration** menu.
2. Click the **Configure Included Window** radio button.
3. Click **New**.
4. Enter a descriptive name under **Window name**.
5. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position).
6. Adjust the Object size, History and Sensitivity profile sliders (see table below for details). Any detected motion within an active window is then indicated by red peaks in the **Activity** window (the active window has a red frame).
7. Click **Save**.

To exclude parts of the Include window, click the **Configure Excluded Windows** button and position the Exclude window as required, within the Include window.

Please see the online help for descriptions of each available option.

	Object Size	History	Sensitivity
High level	Only very large objects trigger motion detection	An object that appears in the region will trigger the motion detection for a long period	Ordinary colored objects on ordinary backgrounds will trigger the motion detection
Low level	Even very small objects trigger motion detection	An object that appears in the region will trigger motion detection for only a very short period	Only very bright objects on a dark background will trigger motion detection
Default value	Low	Medium to High	Medium to High

Examples:

- Avoid triggering on small objects in the image by selecting a high **object size** level.
- To trigger motion detection as long as there is activity in the area, select a high **history** level.
- To only detect flashing light, low **sensitivity** can be selected. In other cases, a high level is recommended.

Port Status

Under **Event Configuration > Port Status** there is a list showing the status for the camera's input and output. This is for the benefit of **Operators**, who cannot access the System Options section.

Example: If the Normal state for a door push button connected to an input is set to **Open circuit –** as long as the button is not pushed, the state will be **inactive**. If the doorbell button is pushed, the state of the input changes to **active**.

System Options

Security - Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:

Users - the **user list** displays the authorized users and access levels:

- **Viewer** - the lowest level of access, which only allows the user access to the Live View page.
- **Operator** - an Operator can view the Live View page, create and modify event types and adjust certain other settings. The Operator does not have access to the Systems Options configuration pages.
- **Administrator** - an administrator has unrestricted access to the Setup Tools and can determine the registration of all other users.

To add a new user, click the **Add...** button and see the online help.

User Settings - check the relevant checkboxes to enable:

- **Enable anonymous viewer login** - allows any viewer direct access to the Live View page.
- **Maximum number of simultaneous viewers** - enter a value here to restrict the number of unicast viewers accessing the unit. This is useful if you need to save on bandwidth. (Note that all multicast viewers count as 1 viewer.)

Note: The AXIS 221 keeps a log of all users that access it. See *Logs & Reports*, on page 44.

Security - IP Address Filtering

Checking the **Enable IP address filtering** box enables the IP address filtering function. Up to 256 IP address entries may be specified (a single entry can contain multiple IP addresses). Click the **Add** button to add new filtered addresses.

When the IP address filter is enabled, addresses added to the list are set as allowed or denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, i.e. if the addresses in the list are allowed, then all others are denied access, and vice versa. See also the online help for more information.

Referrals

To prevent unauthorized clients from including the video stream from the cameras into external Web pages, check the **Referrals** checkbox and enter the IP address or Host name of the computer that hosts the Web pages with the included video stream. Several IP addresses/host names can be defined and are separated by semicolons (;). This option is only applicable to Motion JPEG video streams.

Notes:
- If the referrals feature is enabled and you wish to also allow normal access to the Live View page, the product's own IP address or host name must be added to the list of allowed referrers.
- Restricting referrers has no effect on an MPEG-4 video stream. To restrict an MPEG-4 stream, IP address filtering must be enabled.
- Restricting referrers is of greatest value when not using IP address filtering. If IP address filtering is used, then the allowed referrers are automatically restricted to those allowed IP addresses.

Security - HTTPS

The AXIS 221 supports encrypted browsing using HTTPS.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click the **Create self-signed Certificate** button to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security will only be implemented after the installation of a signed certificate issued by a certificate authority.

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking the **Properties...** button. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera.

Please refer to the online help for more information.

Security - 802.1x

IEEE 802.1x is an IEEE standard for port-based Network Admission Control. It provides authentication to devices attached to a network port (wired or wireless), establishing a point-to-point connection. If authentication fails, access is prevented on the port. 802.1x is based on EAP (Extensible Authentication Protocol).

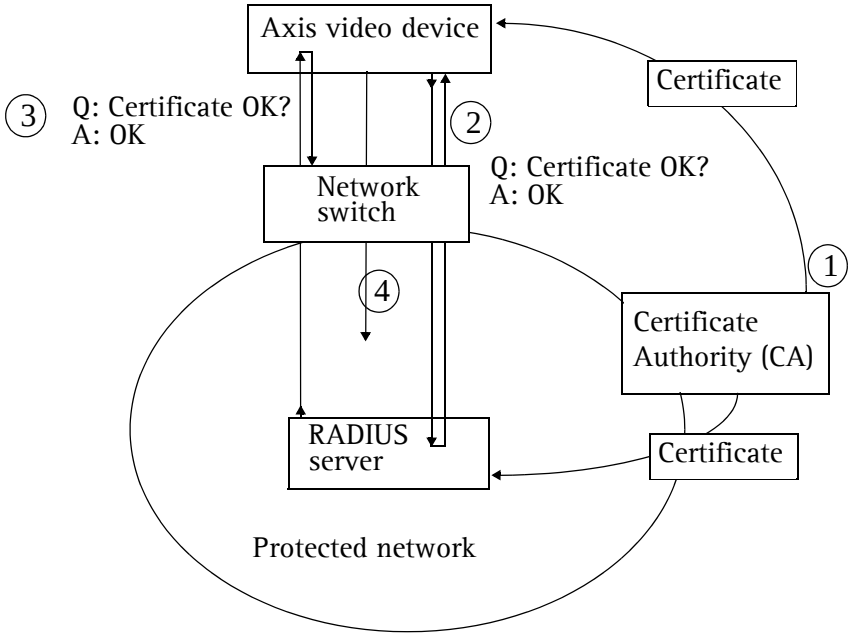
In a 802.1x enabled network switch, clients equipped with the correct software can be authenticated and allowed or denied network access at the Ethernet level.

Clients and servers in an 802.1x network may need to authenticate each other by some means. In the Axis implementation this is done with the help of digital certificates provided by a Certification Authority. These are then validated by a third-party entity, such as a RADIUS server, examples of which are Free Radius and Microsoft Internet Authentication Service.

To perform the authentication, the RADIUS server uses various EAP methods/protocols, of which there are many. The one used in the Axis implementation is EAP-TLS (EAP-Transport Layer Security).

The AXIS network video device presents its certificate to the network switch, which in turn forwards this to the RADIUS server. The RADIUS server validates or rejects the certificate and responds to the switch, and sends its own certificate to the client for validation. The switch then allows or denies network access accordingly, on a pre-configured port.

The authentication process



1. A CA server provides the required signed certificates.

2. The Axis video device requests access to the protected network at the network switch. The switch forwards the video device's CA certificate to the RADIUS server, which then replies to the switch.

3. The switch forwards the RADIUS server's CA certificate to the video device, which also replies to the switch.

4. The switch keeps track of all responses to the validation requests. If all certificates are validated, the Axis video device is allowed access to the protected network via a pre-configured port.

RADIUS

RADIUS (Remote Authentication Dial In User Service) is an AAA (Authentication, Authorization and Accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

CA servers

In cryptography, a Certification Authority (CA) is an entity that provides signed digital certificates for use by other parties, and thus acts a trusted third party.

There are many commercial CA's that charge for their services. Institutions and governments may have their own CA, and there are free CA's available.

Date & Time

Current Server Time - displays the current date and time (24h clock). The time can be displayed in 12h clock format in the Overlay Images (see below).

New Server Time - Select your time zone from the drop-down list. If you want the AXIS 221 clock to automatically adjust for daylight savings time, select the **Automatically adjust for daylight saving time changes**.

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time** - sets the time from the clock on your computer.
- **Synchronize with NTP Server** - the camera will obtain the time from an NTP server every 60 minutes. Specify the **NTP server**'s IP address or host name.
- **Set manually** - this option allows you to manually set the time and date.

Note: Note that if using a host name for the NTP server, a DNS server must be configured under **TCP/IP** settings. See **Network > TCP/IP** below.

Date & Time Format Used in Images - specify the formats for the date and time (12h or 24h) displayed in the Live View video streams.

Use the predefined formats or use your own custom date and time formats. See **Advanced File Naming & Date/Time Formats** in the online help for information on how to create your own file formats.

Network - Basic TCP/IP Settings

IP Address Configuration

The AXIS 221 supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled.

When using IPv4, the IP address can be set automatically via DHCP, or a static IP address can be set manually.

If IPv6 is enabled, your camera will receive an IP address according to the configuration in the network router.

There are also options for setting up notification of changes in the IP address, and for using the AXIS Internet Dynamic DNS Service. For more information on setting the IP address, please see the online help.

Notes:
- To receive notification whenever the camera's IP address changes (via e.g. DHCP), configure the options for notification of IP address change. See **Services** below.
- If your DHCP server can update a DNS server, you can access the AXIS 221 by host name which is always the same, regardless of the IP address.

Services

Enable ARP/Ping setting of IP address - The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Uncheck this box to disable the service in order to prevent unintentional resetting of the IP address. For more information see *Other methods of setting the IP address* in the *AXIS 221 Installation Guide*.

Notes:
- The ARP/Ping service is automatically disabled 2 minutes after the unit is started, or as soon as an IP address is set.
- Pinging the unit will still be possible when this service is disabled.

Options for notification of IP address change - If the IP Address for the camera is changed automatically, e.g. by DHCP, you can choose to be notified of the change. Click **Settings...** and enter the required information.

AXIS Internet Dynamic DNS Service - The AXIS Internet Dynamic DNS Service can provide your Axis product with its own URL (web address), which can then be used to access it over the Internet. The product can be unregistered from the service at any time. To do this click **Settings...** and follow the instructions. For more information, please refer to the online help.

Network - Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.

Obtain DNS server address via DHCP - automatically use the DNS server settings provided by the DHCP server. Click the View button to see the current settings.

Use the following DNS server address - enter the desired DNS server by specifying the following:

- **Domain name** - enter the domain(s) to search for the host name used by the AXIS 221. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, e.g. myserver is the host name in the Fully Qualified Domain Name myserver.mycompany.com where mycompany.com is the Domain name.
- **Primary DNS server** - enter the IP address of the primary DNS server.
- **Secondary DNS server** - will be used if the primary DNS server is unavailable.

NTP Configuration

Obtain NTP server address via DHCP - check this radio button to automatically look up and use the NTP server settings as provided by DHCP. Click the **View** button to see the current settings.

Use the following NTP server address - to make manual settings, check this radio button and enter the host name or IP address of the NTP server.

Host Name Configuration

The AXIS 221 can be accessed using a host name, instead of an IP address. The host name is usually the same as the assigned DNS Name. It is always the first part of a Fully Qualified Domain Name and is always one word, with no period. For example, **myserver** is the host name in the Fully Qualified Domain Name myserver.mycompany.com.

Enabling dynamic DNS updates allows you to alias a dynamic IP address to a static host name, allowing your computer to be more easily accessed from various locations on the Internet. Outside users can always access your server using the associated DNS name regardless of the WAN IP. The DNS server used by the user and/or the DNS server responsible for the domain in use must support RFC2136 and allow updates from the camera.

The **TTL** (Time To Live) value determines how long (in seconds) the reply from the DNS server should be remembered when checking that the domain name for the registered IP address is still valid.

Link-Local IPv4 Address

Link-Local Address is enabled by default and assigns the AXIS 221 with an additional IP address for the UPnP protocol. The AXIS 221 can have both a Link-Local IP and a static/DHCP IP address at the same time - these will not affect each other. See *Network - UPnP™*, on page 42.

HTTP

The default HTTP port number **(80)** can be changed to any port within the range 1024-65535. This is useful for e.g. simple port mapping.

HTTPS

The default HTTPS port number **(443)** can be changed to any port within the range 1024-65535. HTTPS is used to provide encrypted web browsing.

NAT Traversal

Use NAT traversal when your AXIS 221 is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router will be forwarded to the network camera.

Enable/Disable - When enabled, the AXIS 221 will attempt to configure port mapping in a NAT router on your network, using UPnP™.

Use manually selected NAT router - Select this option to manually select a NAT router. Enter the IP address for the router in the field provided.

If a router is not manually specified, the AXIS 221 will automatically search for NAT routers on your network. If more than one router is found, the default router, specified in **System Options > Network > TCP/IP > Basic > IPv4 Address Configuration > Default router**, will be selected.

Alternative HTTP port - Select this option to manually define an external HTTP port. Enter the port number in the field provided. If no port is entered here a port number will automatically be selected when NAT traversal is enabled.

FTP

The FTP server running in the AXIS 221 enables the upload of e.g. new firmware, user applications, etc. Check the box to enable the service.

RTSP

The RTSP protocol allows a connecting client to start an MPEG-4 stream. Enter the RTSP port number to use. The default setting is 554.

Network Traffic

Connection type - The default setting is **Auto-Negotiate**, i.e. the correct speed is automatically selected. If necessary, the connection speed can be set by selecting it from the drop-down list.

Maximum bandwidth - Specify, in Mbit/s or kbit/s, the maximum bandwidth that the camera is allowed to use on the network. This is a useful function when connecting the camera to busy or heavily loaded networks. The default setting is **Unlimited**.

Note: When using MPEG-4 as the video format, remember that setting a maximum bandwidth value here may create problems for individual video streams if the maximum value is less than the sum of the bit rates set for the video streams.

For more information, please see the online help.

Network - SOCKS

SOCKS is a network proxy protocol. The camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server. This functionality is useful if the camera is located on a local network behind a firewall, but notifications, uploads, alarms, etc., need to be sent to a destination outside the local network (e.g. to the Internet).

Network - QoS (Quality of Service)

Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as e.g. a maintained level of bandwidth, low latency, no packet losses, etc. The main benefits of a QoS-aware network can be summarized as:

- the ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to e.g. reserve a fixed amount of bandwidth for these types of traffic. The following types of traffic are marked:

- live video
- event/alarm traffic
- management network traffic

It is important to remember that to be able to use QoS, your network must be properly configured. If you are unsure as to whether your network is QoS aware, please check with your network administrator.

QoS Settings

For each type of network traffic supported by your Axis network video product, enter a DSCP (Differentiated Services Codepoint) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it.

Note that DSCP values can be entered in decimal or hexadecimal form, but saved values are always shown in decimal.

For more information on Quality of Service, please see the Axis support web at www.axis.com/techsup

Network - SMTP (email)

Enter the host names or addresses for your primary and secondary mail servers in the fields provided, to enable the sending of event and error email messages from the camera to predefined addresses via SMTP.

Network - SNMP

The Simple Network Management Protocol (SNMP) allows the remote management of network devices. Select the version of SNMP to use, depending on the level of security required. HTTPS should be enabled when setting the password for SNMPv3.

Network - UPnP™

The camera includes support for UPnP™, which is enabled by default. If also enabled on your computer, the camera will automatically be detected and a new icon will be added to "My Network Places."

Note: UPnP must also be enabled on your Windows XP or ME computer. To do this, open the Control Panel from the **Start Menu** and select **Add/Remove Programs**. Select **Add/Remove Windows Components** and open the **Networking Services** section. Click **Details** and then select **UPnP** as the service to add.

Network - RTP (Multicast)/MPEG-4

These settings are the IP address, port number, and Time-To-Live value to use for the video stream(s) in multicast MPEG-4 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help.

Network - Bonjour

The AXIS 225FD includes support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support Bonjour.

Ports & Devices

I/O Ports

The two alarm inputs and one output on the AXIS 221 can be connected to various external devices, e.g. door sensors and alarm bells. The name given to the ports can be changed and state of the I/O ports can be set to **Open circuit** or **Closed circuit**.

The pinout, interface support and the control and monitoring functions provided by this connector are described in *Unit Connectors,* on page 46.

COM Ports RS-485/422 & RS-232

The RS-485/422 and RS-232 connectors can also be configured to allow them to be controlled by TCP/IP applications. The TCP/IP parameters are described in the online help.

It is possible to configure COM Ports RS-485/422 and RS-232 for Pan/Tilt/Zoom (PTZ) functionaliy, but only with additional third party hardware and a compatible PTZ driver. For more information, please contact support at www.axis.com

LED Settings

The Status and Network Indicator LEDs can be set to flash at a configurable interval (or to not light up at all) whenever the unit is accessed. For a listing of all LED behavior, see page 7, or the online help.

Note: The LED does not flash when the stream is retrieved using MPEG-4 multicast.

Maintenance

- **Restart** - The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
- **Restore** - The unit is restarted and most current settings are reset to the factory default values. The only settings saved are:
  - the boot protocol (DHCP or static)
  - the static IP address
  - the default router
  - the subnet mask
  - the system time
- **Default** - The Default button should be used with caution. Pressing this button will return all of the camera's settings, including the IP address, to the factory default values. The camera will then have to be re-installed.

Upgrade Server - See *Upgrading the Firmware*, on page 50.

Backup - To take a backup of all of the parameters, and any user-defined scripts, click the **Backup** button. If necessary, it is then possible to return to the previous settings if the settings are changed and there is unexpected behavior.

Restore - Click the **Browse** button to locate the saved backup file (see above) and then click the **Restore** button. The settings will be restored to the previous configuration.

Note: **Backup** and **Restore** can only be used on the same unit running the same firmware. This feature is not intended for the configuration of multiple units or for firmware upgrades.

Support

Support Overview

The **Support Overview** page provides valuable information on troubleshooting and contact information, should you require technical assistance.

System Overview

The **System Overview** page provides an overview of the current network, security, event and camera settings.

Logs & Reports

When contacting Axis support, please be sure to provide a valid Server Report with your query. The Access Log is automatically included in the server report.

Information

This page gives you access to the following log files and reports that may prove useful when troubleshooting a problem or when contacting the Axis support web.

System Log - Provides information about system events.

Access Log - The **Access Log** may be used for various purposes:

- Security - Tracking all access to your the camera. The access log lists the IP addresses, users and networking protocols used to access the camera.
- Simple web attraction tracker.
- System analysis and trouble shooting.

Server Report - Provides information about the server status and should always be included when requesting support.

Parameter List - Shows the unit's parameters and their current settings.

Connection List - Lists all clients that are currently accessing video and audio. It is also used for system analysis and trouble shooting.

Configuration

From the drop-down lists, select the size and level of information to be added to the **System** and **Access Log** files.

The default information level for the **Access Log** is set to **Critical & Warnings**. However, in an error situation and when requesting support, set it to the lowest information level **Critical & Warnings & Info**.

For the **Log Level for Email**, select from the drop-down list the level of information to send as email and enter the destination email address.

Advanced

Scripting is an advanced function that provides the means for customizing and using scripts.

Caution!

The scripting function is a very powerful tool. Improper use may cause unexpected behavior or even loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings (in which case, a previously saved backup file will be useful for returning the unit to its latest configuration).

Axis strongly recommends that you do not use this function unless you fully understand its consequences. Axis support provides no assistance for customized scripts.

For more information, please visit the Developer pages at www.axis.com/developer

Plain Config - this function is for the advanced user with previous experience of configuring Axis cameras. All parameters can be set and modified from this page. Help is available via the links on the standard setup pages.

About

Third Party Software Licenses - click View licenses for a list of the licensed software used in the AXIS 221.

Resetting to the Factory Default Settings

To reset the camera to the original factory default settings, go to the **System Options > Maintenance** web page (as described in *Maintenance,* on page 43) or use the **Reset button** (see the illustration in *Overview,* on page 6) as described below:

Using the Reset Button

To reset the camera to the factory default settings using the Control Button:

1. Disconnect the power adapter, or the network cable if using PoE.
2. Press and hold the Control button while reconnecting power.
3. Keep the Control button pressed until the **Status Indicator** color changes to amber (which may take up to 15 seconds).
4. Release the Control button.
5. When the Status Indicator changes to Green (which may take up to 1 minute), the process is complete and the camera has been reset. The unit will now have the default IP address 192.168.0.90 if you are not using a DHCP server.

Unit Connectors

This section describes the following:

- The I/O Terminal connector
- Power connections
- The RS-232 D-Sub connector

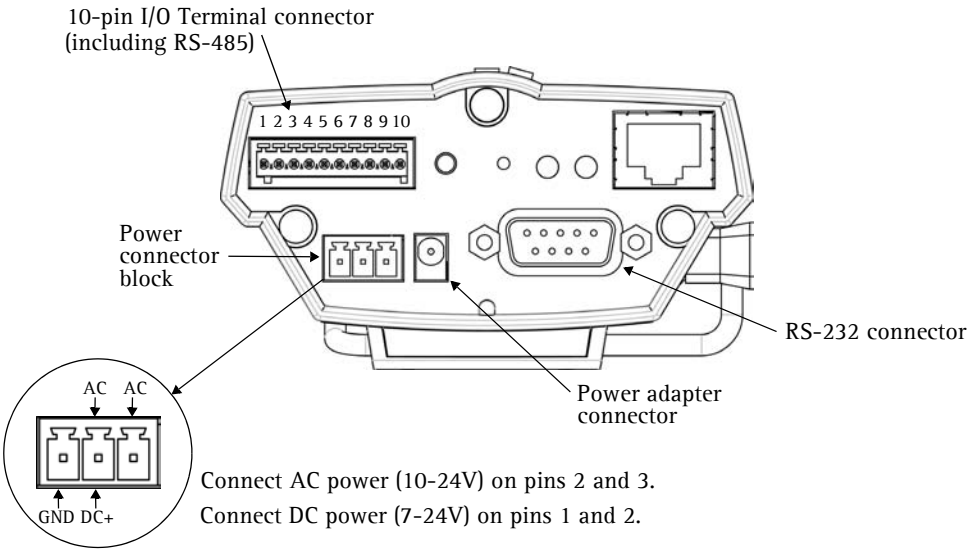
I/O Terminal connector

The 10-pin I/O terminal connector provides the interface to a solid state relay output, two digital photo-coupled inputs, RS-485, GND and auxiliary power.

The terminal connector is used in applications for e.g. motion detection, event triggering, time lapse recording, alarm notification via e-mail, image storage to FTP locations, etc.

- **Input** - Used for connecting external alarm devices and triggering images for specific alarm-based events. The input is typically connected to a motion detector or any other external security device, and images can be uploaded whenever the detector is activated. Maximum 18V DC is allowed on the input.
- **Output** - This can drive a maximum load of 50V DC at 100mA directly or heavier loads by connecting additional relay circuitry. If the output is used with an external relay, a diode must be connected in parallel with the load for protection against any voltage transients.

Caution!
Connecting AC to the inputs/outputs will damage the unit.

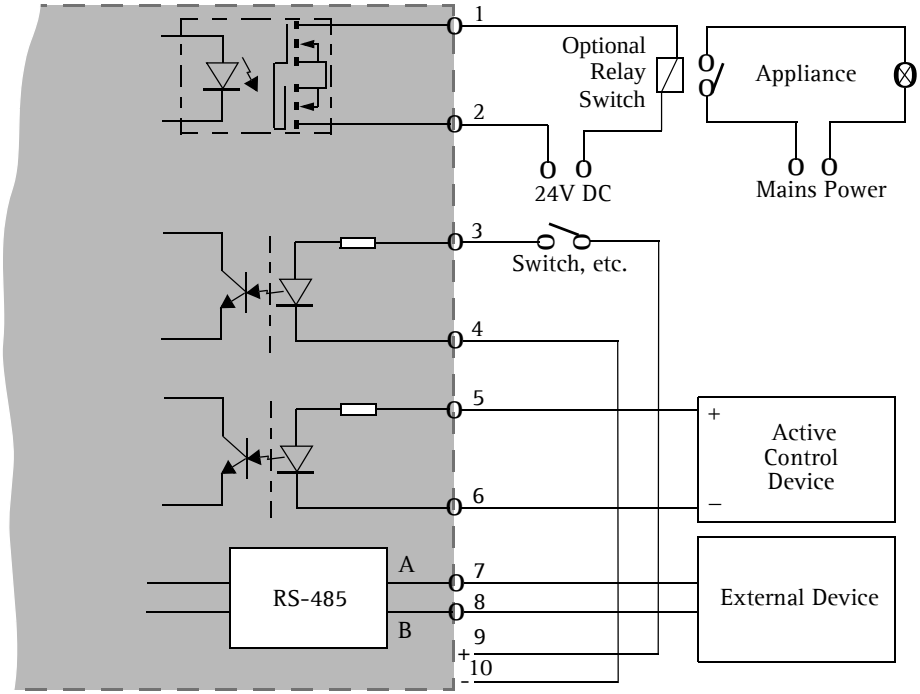


I/O terminal connector pinout table

Pin	Function	Description
1	Output A	On the external device output terminals (A and B), there is no distinction between positive and negative (+ and -). The terminals use a photocoupler and are electrically isolated from the other internal circuitry. The maximum load should not exceed 100mA and the maximum voltage should be not more than 50V DC. Note: Connecting AC to the output will damage the unit.
2	Output B	
3	Digital Input 1 Photocoupler Anode (+)	Photocoupled Input 1. Electrically isolated from the chassis and connectors, this input can be supplied from an external DC voltage or the DC Power Input/Output on pins 9 (DC+) and 10 (GND).
4	Digital Input 1 Photocoupler Cathode (-)	
5	Digital Input 2 Photocoupler Anode (+)	Photocoupled Input 2. As above.
6	Digital Input 2 Photocoupler Cathode (-)	
7	RS-485-A (non-inverting)	A half-duplex RS-485 interface for controlling auxiliary equipment.
8	RS-485-B (inverting)	
9	DC + Power Output	This can drive the photocoupler inputs or other equipment. The output voltage level is 3.0 V. A maximum current of 100mA can be sourced from the DC output.
10	GND	Ground.

I/O Terminal connector schematic diagram

Example schematic diagram of the AXIS 221 terminal connector - showing possible applications.



Power connections

Power can be supplied to the camera by the following methods:

- the supplied power adapter, PS-K, 9W. The center pin is positive (+).
- PoE (Power over Ethernet) with power classification Class 2, via the network cable. This will automatically be detected if available via the network.
- the power connector block on the rear panel.

Power connector block

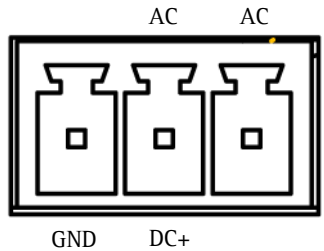
The power connector block supports both AC and DC input power.

The DC supply is 7-24V. Connect the negative pole to the GND pin and the positive pole to the DC+ pin.

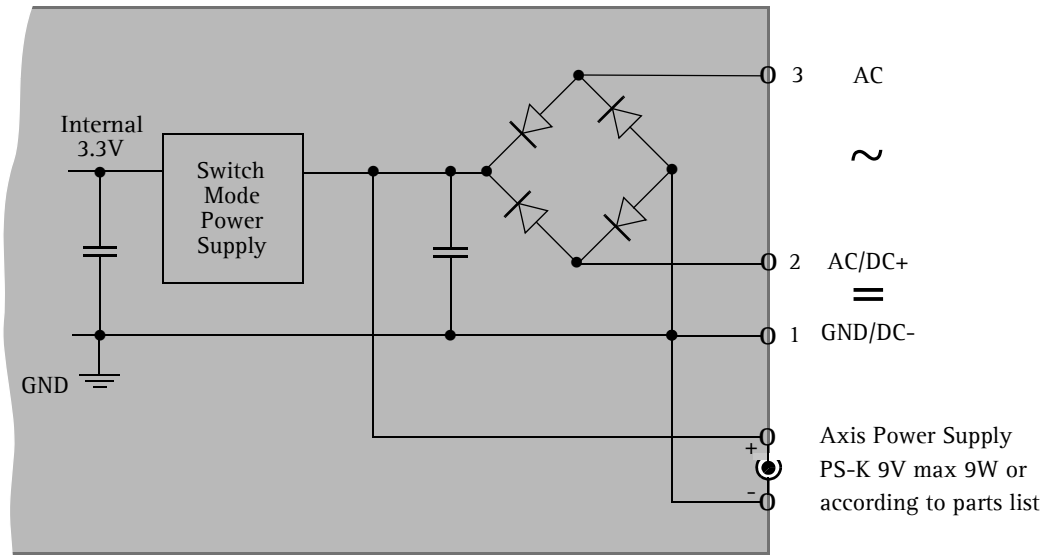
The AC supply is 10-24V. Connect the AC poles to the AC pins.

Power connector block pin assignment table.

Pin	Function
GND	Ground/DC-
AC/DC+	AC and DC+, power input for mains power to unit
AC	AC power input for mains power to unit



Schematic Diagram - Power terminal block and power connectors

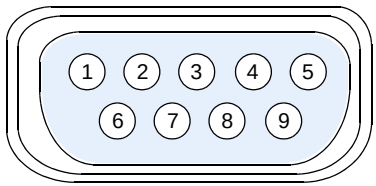


The RS-232 connector

The AXIS 221 provides one 9-pin D-sub connector, providing the physical interface for an RS-232 port, used for connecting accessory equipment.

A diagram of the RS-232 connector, complete with pin assignment table, is shown below.

Pin	Function
1	CD
2	- RXD
3	- TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI



Troubleshooting

Checking the Firmware

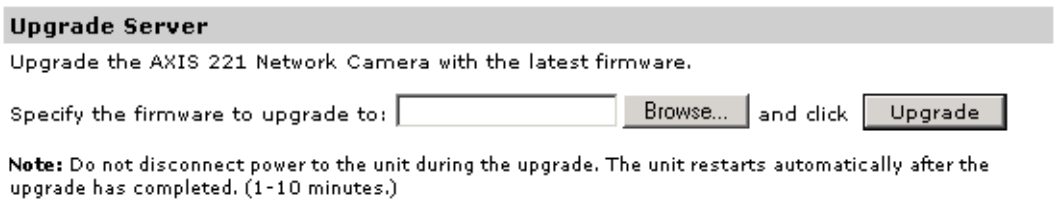
Firmware is software that determines the functionality of the AXIS 221. One of your first actions when troubleshooting a problem should be to check the currently installed firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in your AXIS 221 can be seen on the page **Setup > Basic Configuration.**

Upgrading the Firmware

When you upgrade the firmware with a file from the Axis Web site, your Axis camera will receive the latest available functionality. Always read the upgrade instructions and release notes available with each new release, before updating the firmware.

Note: Preconfigured and customized settings should be saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications.

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from the Axis Web site at **www.axis.com/techsup**
2. Go to **Setup > System Options > Maintenance** in the camera's Web pages.
3. In the **Upgrade Server** section, browse to the desired firmware file on your computer. Click **Upgrade**.


Upgrade Server
Upgrade the AXIS 221 Network Camera with the latest firmware.
Specify the firmware to upgrade to:
Browse...
and click
Upgrade
Note: Do not disconnect power to the unit during the upgrade. The unit restarts automatically after the upgrade has completed. (1-10 minutes.)

Notes:

- If you suspect the firmware upgrade for the AXIS 221 has failed, always wait at least 5-10 minutes before restarting the upgrade process.
- Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.
- Always read the upgrade instructions available with each new release, before updating the firmware.

Emergency Recovery Procedure

If power to the AXIS 221 is lost during the upgrade, the process will fail and the unit will become unresponsive. A flashing red Status LED indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label attached to the bottom of the camera.

1. **UNIX/Linux** - From the command line, type the following:
   arp -s <IP address of AXIS 221> <Serial number> temp
   ping -s 408 <IP address of camera>

   Windows - From a command/DOS prompt, type the following:
   arp -s <IP address of AXIS 221> <Serial number>
   ping -l 408 -t <IP address of camera>
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the camera's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, e.g. axis221.bin. Then click the Load button to restart the upgrade process.
4. After the upgrade has completed (1-10 minutes), the unit will automatically restart and show a steady green on the Power and Status LEDs and flashing green or amber on the Network LED.
5. Reinstall the AXIS 221.
6. **Windows** - From a command/DOS prompt, type the following if you are using a DHCP server:
   arp -d <IP address of AXIS 221>

If the emergency recovery procedure does not get the camera up and running again, please contact Axis support at www.axis.com/techsup/

Axis Support

If you contact Axis support, please help us to help you solve your problems, by providing the server report, the log file and a brief description of the problem.

Server Report - go to **Setup > System Options > Support Overview**. The server report contains important information about the server and its software, as well as a list of the current parameters.

The **Log file** is available from **Setup > System Options > Logs & Reports**. The Log file records events in the unit since the last system restart and can be a useful diagnostic tool when troubleshooting.

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address

When using ARP/Ping.	Try the installation again. The IP address must be set within two minutes after running the ARP command. Ensure the Ping length is set to 408.
The camera is located on a different subnet.	If the IP address intended for the AXIS 221 and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device.	Disconnect the AXIS 221 from the network. Run the Ping command. (In a Command/DOS window, type **ping** and the **IP address** of the unit). If you receive: **Reply from <IP address>: bytes = 32; time = 10 ms.....** - this means that the IP address is already in use on your network. You must obtain a new IP address and reinstall the unit. If you see: **Request timed out** - this means that the IP address is available for use with your camera. In this case, check all cabling and reinstall the unit.
Possible IP address conflict with another device on the same subnet.	The static IP address in the AXIS 221 is used before the DHCP server sets a a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the camera. To avoid this, set the static IP address to 0.0.0.0.

The AXIS 221 cannot be accessed from a Web browser

The IP address has been changed by DHCP.	1) Move the AXIS 221 to an isolated network, or to one with no DHCP or BOOTP server. Set the IP address again, using the AXIS IP Utility (see the Installation Guide) or the ARP/Ping commands. 2) Access the unit and disable DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit will now have a dynamic IP address, but will notify you if the address changes.
Proxy server.	If using a proxy server, try disabling the proxy setting in your browser.
Other networking problems.	Test the network cable and connectors by connecting it to another network device, then Ping that device from your workstation. See the instructions above.
Cannot log in.	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type in http or https in the browser's address bar.
Incorrect host name.	Check that the host name and DNS server settings are correct. See the basic and advanced TCP/IP settings.

Cannot send notifications, uploads, alarms, etc, to a destination outside the local network

Firewall protection.	The camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server.

Your AXIS 221 is accessible locally, but not externally

Firewall protection.	Check the Internet firewall with your system administrator.
Default routers required.	Check if you need to configure the default router settings.

Poor or intermittent network connection

Network switch.	If using a network switch, check that the port on that device uses the same setting for the network connection type (speed/duplex) as set in the advanced TCP/IP settings. The Auto-Negotiate setting is recommended.

Video/Image problems – general

No images in browser (*Internet Explorer for Windows only*)	To enable the updating of video images in Microsoft Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control (AMC) component is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited.	Configure your AXIS 221 to use a Java applet for updating the video images under Live View Config > Layout > Default Viewer for Internet Explorer. See the online help for more information.
Image too dark or too light.	Check the video image settings. See the online help on Video and Image Settings.
Missing images in uploads.	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update.	Configuring, e.g. pre-buffers, motion detection, high-resolution images, high frame rates, etc, will reduce the performance of the camera.
Poor performance.	Poor performance may be caused by e.g. heavy network traffic, multiple users accessing the unit, low performance clients, use of features such as Motion Detection, Event handling, Image rotation other than 180 degrees.
Image gradually gets darker or lighter.	When using the AXIS 221 in locations lit by fluorescent lighting, check in the advanced image settings that the Exposure control is set to **Flicker-free**.
Image loses focus often.	Disable the DC-Iris lens in the settings for **Video & Image > Advanced**. Focus the camera following the instructions on page 9, and then enable the DC-Iris lens.
Images only shown in black & white.	Check the color level setting. Check the setting for the IR cut filter. Images are shown in color only when this filter is enabled, i.e. when set to yes or auto.
Blurred images.	Refocus the camera. Check in the Video & Image > Advanced - Camera Settings that DC-Iris is set to Enabled. If the images are still blurred adjust the metal ring until the image is sharp, see *Removing and attaching the lens,* on page 55.
Rolling dark bands or flickering in image.	Try adjusting the Flicker-free exposure setting under advanced image settings. Note that the 'Hold Current'/Manual setting may cause unwanted effects.

Video/image problems – MPEG-4

Lower frame rate than expected.	Check with the administrator that there is enough bandwidth available. Check also the settings for bit rate control, in the **Video & Image > Advanced > MPEG-4** settings. Using an inappropriate video object type can also affect the frame rate. See the online help for more information. Check in the AMC control panel applet (MPEG-4 tab) that video processing is not set to **Decode only I frames**. Lower the image resolution. Reduce the number of applications running on the client computer.
No MPEG-4 displayed in the client.	Check that the correct network interface is selected in the AMC control panel applet (network tab). Check that the relevant MPEG-4 connection methods are enabled in the AMC control panel applet (network tab). In the AMC control applet, select the MPEG-4 tab and click the button Set to default MPEG-4 decoder.
No multicast MPEG-4 displayed in the client.	Check with your network administrator that the multicast addresses used by the AXIS 221 are valid for your network.
Multicast MPEG-4 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL (Time To Live) value may need to be increased.

Poor rendering of MPEG-4 images.	Color depth set incorrectly on clients. Set to 16-bit or 32-bit color. If text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering. This is done on the MPEG-4 tab in the AMC control panel applet. Ensure that your graphics card is using the latest device driver. The latest drivers can usually be downloaded from the manufacturer's web site. If images are degrading, try decreasing the GOV length, see *Advanced settings*, on page 20.
Color saturation is different in MPEG-4 and Motion JPEG.	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
The test image does not display as expected	
Image settings.	Not all settings have an effect on the test image. For more information, see the help for Image Settings.
The Power indicator is not constantly lit	
Faulty power supply.	Check that you are using an AXIS PS-K power supply.
The Status and Network indicator LEDs are flashing red rapidly	
Hardware failure.	Contact your Axis dealer.
The Status indicator LED is flashing red and the camera is inaccessible	
A firmware upgrade has been interrupted or the firmware has otherwise been damaged.	See the *Emergency Recovery Procedure*, on page 51 above.
Poor quality snapshot images	
Screen incorrectly configured on your workstation.	In Display Properties, configure your screen to show at least 65000 colors, i.e. at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Browser freezes	
Netscape 7.x or Mozilla 1.4 (or later) can sometimes freeze on a slow computer.	Lower the image resolution.
Problems uploading files	
Limited space.	There is only limited space available for the upload of your own files. Try deleting one or more existing files, to free up space.
Missing images in uploads.	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Overlay is not displayed	
Incorrect size or location of overlay.	The overlay may have been positioned incorrectly. Refer to the online help for information on the limitations when using image overlays and privacy masks.
Motion Detection triggers unexpectedly	
Changes in luminance.	Motion detection is based upon changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be mistakenly triggered. Lower the sensitivity setting to avoid problems with luminance.

For additional assistance, please contact your reseller or see the support pages on the Axis Website at www.axis.com/techsup

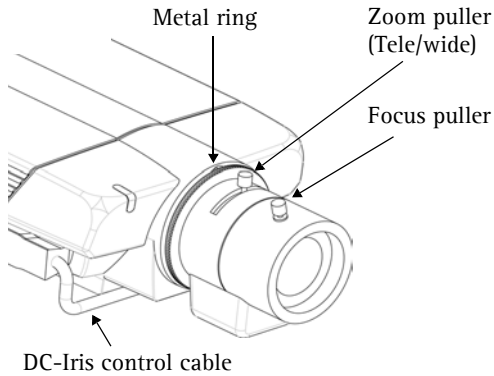
Replacing the lens

If the lens on the AXIS 221 needs to be replaced or if the camera was supplied without a lens, a new lens can be fitted quickly and easily. As the AXIS 221 is designed with a CS-mount, the lens supplied with your product can be replaced with any standard C or CS lens.

Note: Although the lens supplied with your product can be directly replaced with any CS-type lens, a C-type lens must be installed with an adapter for it to work with your AXIS 221. An adapter effectively moves the lens 5mm farther from the camera.

Removing and attaching the lens

1. Disconnect the power supply to the AXIS 221.
2. Disconnect the DC-Iris cable.
3. Unscrew the lens by turning it anti-clockwise.
4. Screw on the new lens until it is tight against the metal ring at the back.
5. Attach the DC-Iris cable to the camera and reconnect the power supply.
6. To focus the new lens, see *Focusing,* on page 9.



Note: In the unlikely case that the camera images are still blurred after focusing the lens, loosen the screw on the underside of the camera that holds the metal ring in place. Turn the metal ring in small increments until a sharp image is obtained. Tighten the screw on the underside of the camera.

Technical Specifications

Item	Specification
Image sensor	1/3" Sony Wfine progressive scan RGB CCD
Lens	• Pentax TS3V310ED • F1.0 varifocal 3.0 - 8.0 mm • DC-iris, • focus range: 0.3 m to infinity • CS mount
Angle of view	• Horizontal: 35° - 93°
Minimum illumination	• Color mode: 0.65 lux, F1.0 • Black and white mode: 0.08 lux, F1.0
Video compression	• Motion JPEG • MPEG-4 Part 2 (ISO/IEC 14496-2), Profiles: ASP and SP
Resolutions	• 16 resolutions from 640 x 480 to 160 x 120 via API, • 5 selections via configuration web page
Frame rate	• Motion JPEG: Up to 45 fps at 640x480 Up to 60 fps at 480x360 or lower • MPEG-4: Up to 30 fps at 640x480 Up to 60 fps at 320x240 or lower
Video streaming	• Simultaneous Motion JPEG and MPEG-4 • Controllable frame rate and bandwidth • Constant and variable bit rate (MPEG-4)
Image settings	• Compression levels: 11 (Motion JPEG)/23 (MPEG-4) • Rotation: 90°, 180°, 270° • Configurable: color level, brightness, sharpness, contrast, white balance, exposure control, exposure area, backlight compensation, fine tuning of behavior at low light • Overlay capabilities: time, date, privacy mask, text or image
Shutter time	2 sec to 1/25000 sec
Security	• Multiple user access levels with password protection • IP address filtering, HTTPS encryption • IEEE 802.1X Network access control • User access log
Users	• 20 simultaneous users • Unlimited number of users using multicast (MPEG-4)
Alarm and event management	• Events triggered by: video motion detection, tampering detection, temperature limits, external input or according to a schedule • Image upload over FTP,email and HTTP • Notification over TCP, email, HTTP and external output 9 MB of pre- and post alarm buffer

Item	Specification
Connectors	• RJ-45 for Ethernet 10BaseT/100BaseTX (PoE) • Terminal block for 2 alarm inputs, 1 output, • RS-485/422 half duplex port and alternative DC power connection • D-sub for RS-232 port
Casing	• Aluminum casing
Processors and memory	• CPU: ETRAX 100LX • Video processing and compression: ARTPEC-2 chip • RAM: 32 MB, • Flash: 8 MB • Battery backed up real-time clock
Power	• 7-24 V DC, max 5.5 W • 10-24 V AC, max 7.5 VA • Power over Ethernet (IEEE 802.3af) Class 2
Operating conditions	• 0 - 50 °C (41 – 122 °F) • Humidity 20 - 80% RH (non-condensing)
Installation, management and maintenance	• AXIS Camera Management tool on CD and web-based configuration • Configuration of backup and restore • Firmware upgrades over HTTP or FTP, firmware available at www.axis.com
Video access from Web browser	• Camera live view, • Video recording to file (ASF) • Sequence tour for up to 20 Axis video sources • Customizable HTML pages
Minimum web browsing requirements	Pentium III CPU 500 MHz or higher, or equivalent AMD,128 MB RAM, AGP graphics card 32 MB RAM, Direct Draw Windows Vista, XP, 2000, DirectX 9.0 or later Internet Explorer 6.x or later For other operating systems and browsers see www.axis.com/techsup
System integration support	• Open API for software integration available at www.axis.com including AXIS VAPIX API • AXIS Media Control SDK • Event trigger data in video stream and access to serial port peripherals over TCP • Quality of Service (QoS) Layer 3 • DiffServ Model • Watchdog • Embedded Linux operating system
Supported protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS*, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, Bonjour, ARP, DNS, DynDNS, SOCKS, NTP etc. More information on protocol usage available at www.axis.com * This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)

Item	Specification
Included accessories	• Installation Guide, CD with User's Manual • installation and management tools • demo software • mounting and connector kits • camera stand • power supply 9 V DC • Single user decoder licenses • MPEG-4 decoder (Windows)
Applications (not included)	• AXIS Camera Station - Video management software for viewing, recording and archiving up to 25 cameras See www.axis.com/partner/adp_partners.htm for more software applications via partners
Accessories (not included)	• Housings for adverse indoor/outdoor environments • Power over Ethernet midspans • IR Illuminators • Network Video Decoder for monitors • MPEG-4 Decoder mulit-user license pack
Approvals - EMC	• EN 55022 Class B • EN 61000-3-2 • EN 61000-3-3 • EN 55024 • EN 61000-6-1 • EN 61000-6-2 • FCC Part 15 Subpart B Class B • ICES-003 Class B • VCCI Class B • C-tick AS/NZS CISPR22 • EN 60950 • Power supply: EN 60950, UL, CSA
Dimensions (HxWxD) and weight	49 x 88 x 186 mm (1,9" x 3,5" x 7,3") 550 g (19,4 oz) excl. power supply

General performance considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some will affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

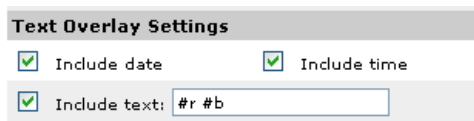
The following factors are among the most important to consider:

- High image resolutions and/or lower compression levels result in larger images. Bandwidth affected.
- Access by large numbers of Motion JPEG and/or unicast MPEG-4 clients. Bandwidth affected.
- Simultaneous viewing of different streams (resolution, compression, etc.) by different clients. Frame rate and bandwidth affected.
- Accessing both Motion JPEG and MPEG-4 video streams simultaneously. Frame rate and bandwidth affected.
- Heavy usage of event settings affects the camera's CPU load. Frame rate affected.
- Enabled motion detection. Frame rate and bandwidth affected.
- Heavy network utilization due to poor infrastructure. Bandwidth is affected.
- Viewing on poorly performing client PC's lowers perceived performance. Frame rate affected.

Optimizing your system

To see the bandwidth and frame rate currenty required by the video stream, the AXIS 221 provides a tool that can be used to display these values directly in the video image.

To do this, special format strings are added as part of a text overlay. Simply add **#r** (average frame rate in fps) and/or **#b** (average bandwidth in kbps) to the overlay.



For detailed instructions, please see the online help for **Video & Image > Overlay Settings**, and the help for **File Naming & Date/Time Formats**.

Important!

- The figures displayed here are the values as delivered by the camera. If other restrictions are currently in force, (e.g. bandwidth limitation) these values might not correspond to those actually received by the client.
- For Motion JPEG, these values will only be accurate as long as no frame rate limit has been specified.

Frame rates - Motion JPEG and MPEG-4

The following table shows typical frame rates in frames/second (fps) for Motion JPEG and MPEG-4 video streams from the AXIS 221.

Note that these values are guidelines only - actual values may vary.

Motion JPEG settings:

- Viewing in AMC
- Compression level = 30%

MPEG-4 settings:

- Viewing in AMC
- Compression level = 30%
- Video Object Type = Advanced Simple
- GOV length = 8
- GOV structure = IP*

*Note that setting the GOV structure to use "I-frames only" will increase the frame rate at the expense of the bit rate.

	Frame rates	
	Motion JPEG	MPEG-4
640x480	45	30
480x360	60	45
320x240	60	60
160x120	60	60

Bandwidth

As there are many factors that affect bandwidth, it is very difficult to predict the required amounts. The settings that affect bandwidth are:

- the image resolution
- the image compression
- the frame rate
- the MPEG-4 object type
- the MPEG-4 GOV structure
- the maximum exposure time.

There are also factors in the monitored scene that will affect the bandwidth. These are:

- the amount of motion
- the image's complexity
- the lighting conditions.

For MPEG-4, if there is only limited bandwidth available, and if this is more important than the image quality, using a constant bit rate (CBR) is recommended. Use a variable bit rate (VBR) if the image quality needs to be maintained at a higher level. If supported on the network, consider also using MPEG-4 multicasting, as the bandwidth consumption will be much lower.

Glossary of Terms

ActiveX - A software component, also refered to as a control, that integrates into and extends the Microsoft(R) Internet Explorer(TM) web browser. ActiveX controls are typicaly downloaded and installed dynamicaly by the browser from a web page.

AMC – AXIS Media Control. The control required for viewing video images in Internet Explorer. Installs automatically on first use.

API – Application Programming Interface. The Axis API can be used for integrating Axis products into other applications.

ARP - Address Resolution Protocol. A protocol used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to find out what the MAC address is for the IP address.

ARTPEC - Axis Real Time Picture Encoder - used for video image compression.

CCD - Charge Coupled Device. CCD is one of the two main types of image sensors used in digital cameras. When a picture is taken, the CCD is struck by light coming through the camera's lens. Each of the thousands or millions of tiny pixels that make up the CCD convert this light into electrons.

CGI - Common Gateway Interface. A set of rules (or a program) that allows a Web Server to communicate with other programs.

Client/Server - Describes the network relationship between two computer programs in which one, the client, makes a service request from another - the server.

DC-Iris – This special type of iris is electrically controlled by the Axis camera, to automatically regulate the amount of light allowed to enter.

DNS – The Domain Name System (DNS) locates and translates Internet domain names into IP (Internet Protocol) addresses.

Ethernet - A widely used networking standard.

ETRAX - A family of microprocessors developed by Axis.

Firewall - A virtual barrier between a LAN (Local Area Network) and other networks, e.g. the Internet.

FTP - File Transfer Protocol. Used for the simple transfer of files to and from an FTP-server.

Full-duplex - Transmission of data, e.g. audio, in two directions simultaneously. In an audio system this would describe e.g. a telephone system. Half-duplex also provides bi-directional communication, but only in one direction at a time, as in a walkie-talkie system. See also Simplex.

HTML - Hypertext Mark-up Language. Used widely for authoring documents viewed in web browsers.

HTTP - Hypertext Transfer Protocol. The set of rules for exchanging files (text, images, sound, video, and other files) on the World Wide Web.

HTTPS - Hypertext Transfer Protocol over Secure Socket Layer. A web protocol that provides encryption for page requests from users and for the pages returned by the web server.

Intranet - A private network limited to an organization or corporation. Usually closed to external traffic.

IP - Internet-Protocol. See TCP/IP.

IP address - A unique number used by a network device, to allow it to be identified and found on the network. The 32-bit IP address is made up of four groups (or quads) of decimal digits separated by periods. An example of an IP address is: 192.168.0.1

ISMA - Internet Streaming Media Alliance.

JPEG - A standard image format, used widely for photographs. Also known as JPG.

LAN - A local area network (LAN) is a group of computers and associated devices that typically share common resources within a limited geographical area.

Linux - A popular, free, open source, UNIX like operating system, developed in cooperation by various individuals and organizations.

Lux - A standard unit for the measurement of light, where 1 Lux equals the light emitted from a single candle at a distance of one meter.

Mbit/s - Megabits per second. A unit for measuring speeds in networks. A LAN might run at 10 or 100 Mbit/s.

MPEG-4 - A video compression standard that makes good use of bandwidth, and which can provide high-quality video streams at less than 1 Mbit/s.

Multicast - A bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.

NTSC - National Television Standards Committee. NTSC is the standard format used for televisions in most of North and Central America, and Japan.

NWAY - A network protocol that automatically negotiates the highest possible common transmission speed between two devices.

PAL - Phase Altering Line. PAL is the standard format used for televisions in most of the world (other than the US, Canada, and Japan).

PEM - Privacy Enhanced Mail. An early standard for securing electronic mail. The PEM-format is often used for representing an HTTPS certificate or certificate request.

Ping - A small utility used for sending data packets to network resources to check that they are working and that the network is intact.

Pre/post alarm image - The images from immediately before and after an alarm.

Privacy mask - An image or specified area used to block out certain parts of the video image.

Protocol - A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication, and there are hardware protocols and software protocols.

Router - A device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router is often included as part of a network switch (see below).

RTP - Real-Time Transfer Protocol. A transfer protocol designed for delivery of live contents, e.g. MPEG-4.

Simplex - In simplex operation, a network cable or communications channel can only send information in one direction.

SMTP - Simple Mail Transfer Protocol. A protocol used for e-mail transmissions over the Internet.

SNMP - Simple Network Management Protocol. An application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

Subnet Mask - An IP address consists of two components: the network address and the host address. "Subnetting' enables a network administrator to further divide the host part of the address into two or more subnets. The subnet mask identifies the subnet to which an IP address belongs.

Switch - Whilst a simple hub transmits all data to all devices connected to it, a switch only transmits the data to the device it is specifically intended for.

TCP/IP - Transmission Control Protocol/Internet Protocol. A suite of network protocols that determine how data is transmitted. TCP/IP is used on many networks, including the Internet. TCP keeps track of the individual packets of information and IP contains the rules for how the packets are actually sent and received.

UDP - The User Datagram Protocol is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is also known as UDP/IP.

Unicast - Communication that takes place over a network between a single sender and a single receiver.

UPnP™ - Allows the automatic peer-to-peer detection of devices on the network.

URL - Uniform Resource Locator. An "address" on the network.

Varifocal - A varifocal lens provides a wide range of focal lengths, as opposed to a lens with a fixed focal length, which only provides one.

WAN - Wide-Area-Network. Similar to a LAN, but on a larger geographical scale.

Web server - A program on a computer (server) providing the resources (e.g. web pages) requested by the user (client).

Index

A
Access from a Browser 8
Access Log 44
Accessing the Video Stream 14
Action 27
Action Buttons 25
Active/Inactive 25
Administrators 16
Advanced Camera Settings 20
Advanced Simple Profile 12
Alarm 31, 46
AMC Viewer Toolbar 10
ARP/Ping 38
Auxiliary Power 46
AXIS Media Control (AMC) 14

B
Backup 43
Bandwidth 12, 60
Bit Rate 12
Bonjour 42
Buffers 29

C
Camera Tampering 30
CGI Links 25
Configuration 16
Connection List 44
Constant Bit Rate 12
Custom Settings 23

D
DC-Iris 9
Default Button 43
Default Video Format 25
Default Viewer 25
DNS Configuration 38
DNS Server 38
Domain Name 38

E
Emergency Recovery 51
Event Servers 27
Event Types 28
Events 27
External Video 26

F
Factory Default Settings 45
Firmware 50
Focusing 9
Frame Rate 18
FTP Server 27

H
Host Name 39
HTML Examples 26
HTTP API 25
HTTP Server 27
HTTPS 34

I
I/O Ports 42
I/O Terminal Connector 7, 46
Include Windows 31
Input 46
IP Address Filtering 33

L
LED Indicators 7
Lens 55
Lighting Conditions 20
Live View Configuration 23
Live View Page 10, 16
Low Light Behavior 20

M
Maintenance 43
Motion Detection 31
Motion JPEG 12
MPEG-4 12
MPEG-4 Protocols 13
MPEG-4 Settings 21, 42

Multicast 42
Multicasting 13

N
Network Connector 7
Network Settings - Advanced 38
Network Settings - Basic 37
NTP Server 37

O
Other MPEG-4 Clients 15
Output 46
Output Buttons 25
Overlay/Mask 18
Own Home Page 24
Own Web Files 24

P
Password 9
Port Status 32
Ports & Devices 42
Power Adapter Connector 7
Power Connector Block 7
Pre/Post Trigger Buffer 29
Privacy Mask 18
Pulse 10
Pulse Button 25

R
Recovery 51
Referrals 33
Replacing the Lens 55
Reset Button 7
Restart 43
Restore 43
RS-232 Connector 7, 42, 49
RS-485/422 Connector 42
RTP 13
RTSP 13

S
Scheduled Event 27, 29
Security 33
Security - Users 33
Sequence Mode 10, 26
Serial Number 6
Server Time 37
Services 37
Setup Tools 16
Simple Profile 12
Snapshot Button 10
Streaming MPEG-4 13
Support 43
System Options 33

T
TCP Server 27
TCP/IP Settings 37, 38
Technical Specifications 56
Time Mode 37
Triggered Event 27

U
UDP 13
Unicasting 13
Unit Connectors 46
Upgrade Server 43
Upgrading the Firmware 50
Upload Overlay/Mask 19
Uploading Web Files 24
UPnP 42
User List 33
User-defined Links 24

V
Variable Bit Rate 12
Video Streams 12, 18